EXHIBIT R

NETRANGER™

NETWORK SECURITY MANAGEMENT SYSTEM

USER'S GUIDE

Installation, Configuration, and Operation of the NetRanger System

WheelGroup corporation

Release Notes—NetRanger version 1.3.1

The BorderGuard and Encrypted Sleeves

These Release Notes identify changes that must be made to the BorderGuard filter files generated by nrconfig. If these changes are not made, NetRanger will not operate properly in conjunction with encrypted sleeves. These notes are a supplement to the NetRanger Configuration Instructions and Worksheets, which are in Chapter 3 of the *NetRanger User's Guide*.

After you have run the nrconfig utility and entered all the required configuration information, follow the procedures in these notes for applying the DPF sleeves to the IP first filter point rather than the BorderGuard's apply table. These notes include changes to the filter files for BorderGuards running in either router mode or in bridge mode.

The following parameters are used as examples in these Release Notes:

- Local Org ID: 100
- Remote Org ID: 1001
- Remote Sleeves IP Address: 10.10.101.1 (Address of Remote BorderGuard)
- Director IP Address: 10.10.101.2
- Remote Sleeves Netmask: 255.255.255.0 (Netmask of Remote Network)
- Remote machines to send encrypted data to are: 10.10.101.1, 10.10.101.2
- Local NSX IP Address: 10.11.101.2

BorderGuard in Router Mode

Before proceeding with the following steps, ensure that you have entered the correct Sleeve Configuration information in the nrconfig utility and that you have generated and committed the files.

To configure encrypted sleeves for a BorderGuard running in router mode, make the changes outlined below and on the following page to the appropriate files in the /tmp directory (changes to the files are shown in bold type).

1. **Make the following changes to the sleeves.fil file:**

```
filter DPF_100_1001_1
      ip_da in (10.10.101.1, 10.10.101.2)
            set_sleeve S_100_1001_1;
end
filter DPF_FAIL 100_1001_1
      ip_sa in (10.10.101.1,10.10.101.2)
      not sleeve S_100_1001_1
            copy_to 10.11.101.2 35399
            icmp_unreachable fail;
end
filter DPF
      filter DPF_100_1001_1;
      filter DPF_FAIL_100_1001;
end
```

The line **ip_da in (10.10.101.1, 10.10.101.2)** places all data going to these two IP addresses in sleeve S_100_1001_1.

The line **ip_sa in (10.10.101.1, 10.10.101.2)** ensures data coming from these two IP addresses is in the sleeve S_100_1001_1.

In routing mode, the BorderGuard uses the **copy_to** command to pass data to the NSX.

The NSX receives **copy_to** packets for Security Policy in port 35399.

2. **Add the following line to filters.cmd:**

```
ns compile_filter shun.fil
ns compile_filter sleeves.fil
ns compile_filter first.fil
ns compile_filter last.fil
ns compile_filter incom1.fil
#ns compile_filter incom2.fil
#ns compile_filter out1.fil
#ns compile_filter out2.fil
```

The line **`ns compile_filter sleeves.fil`** will compile the filters in the sleeves.fil file.

3. **Add the following line to first.fil:**

```
filter FIRST_FILTER
     filter NETRANGER;
     filter FIRST_SUCCEED;
     filter SHUN;
     filter DPF;
end
```

The line **`filter DPF;`** will allow FIRST_FILTER to call the new DPF filter.

4. **Remove the line `@sleeves.cmd` from the startup file.**

5. **Remove the `sleeves.cmd` file from /tmp.**

BorderGuard in Bridge Mode

To configure encrypted sleeves for a BorderGuard running in bridge mode, follow these steps:

1. **Log in as user root and enter the following command:**

   ```
   /usr/sbin/sysconfig-nsx
   ```

2. **Choose option 3 (Configure Default Router).**

3. **Enter the** br01 **IP Address of the BorderGuard.**

   This directs all of the NSX's data to a virtual interface of the BorderGuard, br01. If the data is not directed at br01, the data will pass through the bridge and will not get encrypted.

1. **Log in as user netrangr, run the nrconfig utility, and enter the correct information into option 8, Sleeve Configuration.**

NOTE

Be sure that you have entered the correct Sleeve Configuration information (nrconfig MAIN MENU, Option 8) and that you have committed the files (nrconfig MAIN MENU, Option 13) before proceeding with the following steps.

2. **Make the changes shown below and on the following pages to the NSC files placed in the /tmp directory.**

   (Changes to the files are shown in bold type.)

The following parameters are used as examples in these Release Notes:

- Local Org ID: 100
- Remote Org ID: 1001
- Remote Sleeves IP Address: 10.10.101.1 (Address of Remote BorderGuard)
- Director IP Address: 10.10.101.2
- Remote Sleeves Netmask: 255.255.255.0 (Netmask of Remote Network)
- Remote machines to send encrypted data to are: 10.10.101.1, 10.10.101.2
- Local NSX IP Address: 10.11.101.2

3. **Make the following changes to the sleeves.fil file:**

```
filter DPF_100_1001_1
      ip_da in (10.10.101.1, 10.10.101.2)
            set_sleeve S_100_1001_1;
end
filter DPF_FAIL 100_1001_1
      ip_sa in (10.10.101.1,10.10.101.2)
      not sleeve S_100_1001_1
            log_to 10.11.101.2 35401
            icmp_unreachable fail;
end
filter DPF
      filter DPF_100_1001_1;
      filter DPF_FAIL_100_1001;
end
```

The line **ip_da in (10.10.101.1, 10.10.101.2)** places all data going to these two IP addresses in sleeve `S_100_1001_1`.

The line **ip_sa in (10.10.101.1, 10.10.101.2)** ensures data coming from these two IP addresses is in the sleeve `S_100_1001_1`.

In bridge mode, the BorderGuard uses the log_to command to send packets to the NSX.

The NSX receives log_to packets for Security Policy in port **35401**.

4. **Add the following line to filters.cmd:**

```
ns compile_filter shun.fil
ns compile_filter sleeves.fil
ns compile_filter first.fil
ns compile_filter last.fil
ns compile_filter incom1.fil
#ns compile_filter incom2.fil
#ns compile_filter out1.fil
#ns compile_filter out2.fil
```

The line **`ns compile_filter sleeves.fil`** will compile the filters in the sleeves.fil file.

5. **Make the following changes to the startup file:**

   - Remove the line **`@sleeves.cmd`** from the file.
   - Add the line **`netsentry apply ip DPF on first`** before the line `netsentry apply macaddr FIRST_FILTER on first`.

6. **Remove the `sleeves.cmd` file from /tmp.**

NOTE

Remember that in Bridge mode you must also apply a filter to the **`local_in`** filter point to protect the BorderGuard from unauthorized access.

7. **Create a file named local.fil in /tmp:**

```
filter LOCAL_POLICY
   not tcp_connect_request
      break;
   tcp_dp in (23)
   ip_sa in (10.10.101.2, 10.11.101.2)
      break;
   any
      log_to NSX_IP_ADDRESS 35401
      icmp_unreachable fail;
end
```

This filter allows only the Director (10.10.101.2) and NSX (10.11.101.2) to telnet to the BorderGuard.

8. **Add the following line to filters.cmd:**

```
ns compile_filter shun.fil
ns compile_filter sleeves.fil
ns compile_filter first.fil
ns compile_filter local.fil
ns compile_filter last.fil
ns compile_filter incom1.fil
#ns compile_filter incom2.fil
#ns compile_filter out1.fil
#ns compile_filter out2.fil
```

The line **ns compile_filter local.fil** compiles the new LOCAL_POLICY filter.

9. **Add the following line to the startup file:**

```
netsentry apply ip LOCAL_POLICY on local_in
```

This line should be added just after the line `netsentry apply macaddr FIRST_FILTER on first`.

After you have made the appropriate changes to the files in the /tmp directory, you can tftp the files to the BorderGuard. Copy all files you either edited or created to the /usr/nr/etc/nsc directory.

NetRanger™

User's Guide

Version 1.3.1

WheelGroup corporation

WheelGroup Corporation has made every effort to ensure that this *User's Guide* is correct and accurate, but reserves the right to make changes without notice at its sole discretion at any time.

The NetRanger System described in this guide is supplied under a license and may be used only in accordance with the terms of such license, and in particular any warranty of fitness of WheelGroup Corporation products for any particular purpose is expressly excluded and in no event will WheelGroup Corporation be liable for any consequential loss.

CONFIDENTIAL. The NetRanger System software is confidential and a trade secret of WheelGroup Corporation. All use, disclosure, and/or reproduction of this software not expressly authorized in writing by WheelGroup Corporation is prohibited. WheelGroup Corporation shall prosecute all unauthorized use, disclosure, and reproduction of this software under the criminal and civil laws.

NetRanger, WheelGroup Corporation, and the WheelGroup logo are trademarks of WheelGroup Corporation. All other product names in this publication are trademarks or registered trademarks of their owners.

Produced in the United States of America.

GETTING HELP

WheelGroup Technical Assistance

Refer to this *User's Guide* whenever you have a problem using the NetRanger System. If you still cannot solve the problem or if you have questions about anything not covered in this guide, you can call WheelGroup Technical Support from 8:00AM to 6:00PM, CST. This assistance is available Monday through Friday (except holidays). You can reach us in any of the following ways:

Telephone	**1-888-942-6762**
FAX	**210-494-6303**
E-Mail	**help@wheelgroup.com**

Please include the following information in your FAX or e-mail message, or have it available if you are calling (use the NetRanger Problem Report Form on the following page to help you gather this information):

- Your customer number and phone number. For e-mail messages, please include your customer number as part of the subject line for your messages.
- A description of the NSX and Director hardware and software you are using, including any network software

  To determine the version number of the Director software and daemons you are using, type the following commands:

  ```
  nrdirmap -?
  /usr/nr/nrvers
  ```

- Your operating system type and version
- A description of the problem, what you were doing when it occurred, and the exact wording of any error messages that you might have received
- If this is a security question, please include all information related to a specific alarm or attacking site.

NetRanger Problem Report Form

Before you call, please have the following information available.

Organization ID:_____ Host ID (of Problem System):_____

Point of Contact:_____ Phone Number:_____

[redacted]

NSX Information (if applicable)

NSX Type:_____ Number of NSC devices connected to NSX:_____

NSC Type (with problem):_____

NSC Serial Number (with problem):_____

Director Information (if applicable)

Platform: HP SPARC

OV Version:_____ Director Version:_____

Problem Description

_____

_____

_____

_____

_____

[redacted]

Are you a monitored site? Yes No Member of WARN? Yes No

IP addresses of involved machines:_____

Do you wish to talk to WheelGroup about Intrusion Control and Response (ICR) consulting? Yes No

Alarm Type:_____

Description of security incident:_____

_____

_____

WheelGroup Corporation
1-888-942-8762
1-210-494-6303 (fax)
e-mail: help@wheelgroup.com

NETRANGER 1.3 ENHANCEMENTS

This section describes enhancements made to the 1.3 release of NetRanger with respect to the following areas:

- **Installation**
- **Director**
- **Communication**
- **NSX**

Installation

Bridge Filter Changes

In order to properly interpret copy_to and log_to packets under bridge mode all references to tl_byte have been changed to tl_data_byte in the files: first.fil, incom1.fil, and incom2.fil. All references to ip_option_present have also been commented out in incom1.fil and incom2.fil because this option is not supported in bridge mode.

Bug Fixes

- The **nrconfig** utility no longer generates an invalid default route under bridge mode.
- The **pkgadd** process no longer changes the usr:grp permissions of the /usr directory to netrangr:netrangr.
- The **pkgadd** process no longer destroys existing configuration information in /usr/nr/bin/sap.

Director

Support for NetView on IBM/AIX

The NetRanger Director now works with 4.1 and later versions of NetView running with 4.1 and later versions of the IBM/AIX operating system.

Discontinued Solaris 2.4 Support

The 1.3 version of NetRanger no longer supports SPARC Solaris version 2.4.

Improved Alarm Performance

The Director has always avoided generating duplicate alarms by scanning the OVwDB before generating an alarm icon. Prior versions of the Director incurred unnecessary processing overhead by unconditionally scanning the OVwDB. The Director now makes sure that the severity level of the alarm equals or exceeds the OpenView display threshold before it scans the OVwDB.

Improved Alarm Consolidation

Prior to the 1.3 release, the Director generated a separate alarm icon for every source port accessed by a ***DNS Request*** and for every src-dst port pair accessed by a ***TCP Port Sweep.*** The Director now generates a single alarm icon for each of these types of events. This dramatically reduces icon and OVwDB clutter as well as improving overall performance under load. Please note that while the Director generates a single icon for each of these types of events, all of the ports accessed by these services are properly logged by *loggerd*.

Single Window for Source and Destination Address Name Resolution

In previous versions of NetRanger, when the **Security→Show→Names** menu option was selected for multiple alarm icons the Director would generate a window for each alarm. The Director now generates a single window with a scrollable display of alarm names.

New Menu Functions

- The **Security→Exclude Alarms** menu option allows you to suppress all of the alarms for a given src-dst pair.
- The **Security→Show Alarm Submap(s)** menu option allows you to display all of alarms associated with a machine or collection without having to traverse its submaps.
- The **Security→Trouble Ticket** menu option allows you to generate a trouble ticket in a Remedy ARS system for the alarm(s) currently selected.
- The Director now supports the OpenView **Manage** and **Unmanage** functions.

SAP Enhancements

- FileMgmt functionality has been extended and simplified.
- Improved instrumentation tokens have been developed for *sapd* Status and Control.
- ***sapr*** queries are more easy to use and generate more meaningful results.
- *loggerd* is now able to process **heavier alarm loads** from multiple sensors by caching records in a write buffer.
- Chapter 5 of this *User's Guide* now contains new ***Installation*** and ***Tutorial*** sections for SAP.

Bug Fixes

- The **Save-To-File** feature no longer fails when an NSX Collection Name contains spaces, which are now automatically promoted to underbars.
- The *nrdirmap* application now properly cleans up orphaned socket(s) before it tries to reestablish communication with *smid* after a failed communication has occurred.
- The Director no longer generates an error message when it tries to Unshun a network or host.

Communication

Repetitive error messages relating to misconfiguration are now consolidated in errors.postofficed. This helps minimize file system usage.

NSX

Passport in Bridge Mode

The 1.3 version of NetRanger now recognizes log_to packets transmitted by a Passport.

Bug Fixes

- NSX sensors now recognize the ***Multiplexor*** series of the BorderGuard.
- **nrstart** now invokes *managed* when started as user *netrangr* under SPARC Solaris.

Modified Signatures

Signature	Modification
2151	Increased size of allowed ICMP traffic
2000-2012	SubSigID now contains ICMP code value

New *Context* Signatures

Signature	Name
2152	ICMP Flood
3105	Sendmail Decode
4050	UDP Bomb
6200	Ident Buffer Overflow
6201	Ident Newline
6202	Ident Improper Request

New *Content* Signatures

- IFS hacks
- rlogin - froot
- ftp USER
- ftp PASS
- ftp RETR
- ftp STOR
- ftp MKD
- ftp RMD
- ftp SITE
- ftp SYST
- ftp CWD ~root
- ftp PORT
- http GET
- Bad URLs
- rexec USER
- rexec PASS
- ident USER
- pop3 USER
- pop3 PASS
- IP Fragment
- Unknown IP Protocol
- Authentication Fail

1 OVERVIEW

NetRanger's Components and Capabilities

What is NetRanger?

NetRanger is a real-time network security management system that detects, analyzes, responds to, and deters unauthorized network activity. The NetRanger architecture supports large-scale information protection via centralized monitoring and management of remote dynamic packet filtering devices that plug into TCP/IP networks. Communication is maintained via WheelGroup Corporation's (WGC) proprietary secure communications architecture. Network activity can also be logged for more in-depth analysis.

As shown in Figure 1.1, NetRanger 1.3.1 consists of the following core systems and subsystems:

- **Network Security eXchange (NSX)**
  - Packet Filtering Device(s)
  - Sensor
- **Communications System**
  - Post Office(s)
  - Encrypted Sleeve
- **Director**
  - Security Management Interface
  - Security Analysis Package

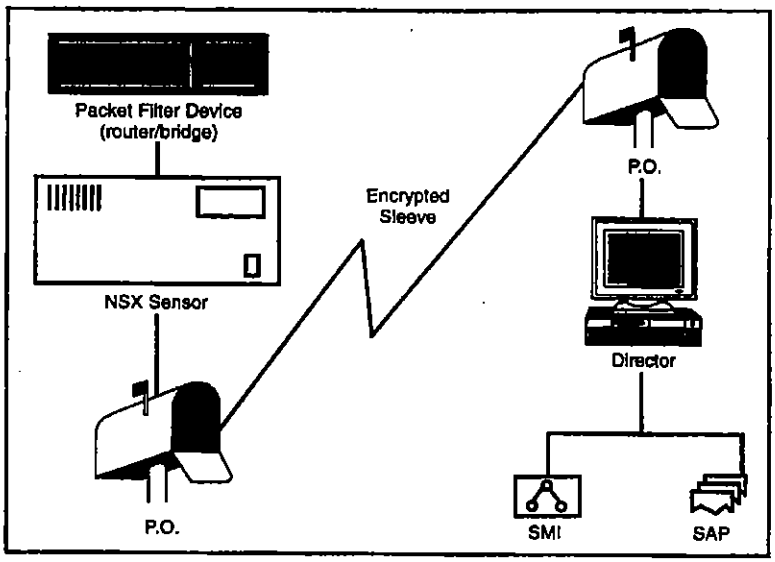

Figure 1.1: Basic NetRanger Components

The NSX

The **NSX** is the sensing and management component of the NetRanger System that resides on a corporate network. It communicates with one or more remote Director systems via the Post Office network communications system. The NSX currently operates with IP networks and supports many hardware and software configuration options.

The **Packet Filtering Device** is a router or bridge that plugs into a corporation's network at a point of entry to other networks. The security policy installed on this device determines what subset of network traffic will be routed to the NetRanger Sensor.

The **Sensor** subsystem contains NetRanger's real-time intrusion detection and content assessment logic. The intrusion detection engine recognizes and responds to attacks, such as sendmail, ping sweeps, IP source routing and spoofing, FTP, and Telnet abuse, and SATAN scans. Sensor analyses produce data streams of IP packets and event records that are either dumped into local session log files or sent on to the Post Office for remote delivery to a Director system. The Sensor also accepts intrusion response and reconfiguration information from Director systems.

The Communication System

The **post office** subsystem provides the communication backbone for remote monitoring and NSX systems management. All communication is based on a proprietary, connection-based protocol that can switch between alternate routes in order to maintain the point-to-point connections specified in its routing tables. All messages are routed based on a three-part address that includes organization, host, and application identifiers.

The **Encrypted Sleeve** secures data transmission between remote protected networks. Encrypted sleeves are currently implemented via the Data Privacy Facility (DPF) that comes with Network Systems Group's (NSG) BorderGuard packet filter devices.

The Director

The **Director** provides monitoring and analysis services to NetRanger, and communicates with one or more NSX systems via the communication system. The Director contains two basic subsystems, the Security Management Interface (SMI) and the Security Analysis Package (SAP).

The **SMI** is a collection of GUIs and tools that help monitor and respond to security events at one or more NSX locations. The SMI integrates with network management applications (such as HP OpenView®). Whereas the SMI is focused primarily on real-time security event management, data analysis is supported by the SAP.

The **SAP** is a set of data analysis tools that analyzes NSX data independently of SMI activities. The SAP consists of three basic components: data collection, data management, and data analysis. Although all components can be easily integrated into an existing SMI platform, WheelGroup recommends that all data be exported onto a separate database server. In this way, the SMI and SAP components can be configured, secured, and tuned independently.

Product Capabilities

One of the attributes that make NetRanger the preeminent intrusion detection and response system is the way in which it integrates many tried and true network security technologies. Most network security applications fall into one of two categories: **firewalls** or **network monitoring**. Both of these technologies suffer from shortcomings not found in NetRanger.

Firewalls represent the most common form of network security, and they gained popularity in part because of their relatively simple host-based installation and friendly graphical user interfaces. The biggest problem with firewalls, however, is that they rely upon *proxy services* to enforce an organization's security policies. Proxy services erect *static* barriers that frequently block legitimate as well as illegitimate activity. This puts

pressure on system administrators to open pathways, which frequently makes firewalls vulnerable to the very events they are supposed to guard against. Because most firewalls are host-based solutions, administration of more than one firewall at a time is also difficult. The system overhead associated with proxy services also prevents most firewalls from being able to scale beyond Ethernet speeds.

Although network monitoring tools can detect unauthorized activities without having to erect barriers to entry, administrators typically have to sift through audit logs after the fact in order to find security breaches. In many instances, systems have been compromised by the time the activity has been detected. Both of these approaches also tend to only look at incoming network traffic.

NetRanger enforces an organization's security policy via **real-time response and detection of intrusive events** without having to erect static barriers. NetRanger's secure communication architecture also allows command and control, as well as system information, to be distributed securely across heterogeneous networks. This section describes these capabilities in a top-down fashion within the context of the underlying architecture.

One of the fundamental design principles of NetRanger is that the *services* required by each of the subsystems be broken apart into their atomic operational components, or *daemons*, which are diagrammed in Figure 1.2. For example, the NetRanger daemon that logs events is totally separate from the ones that perform network sensing and device management. The reasons for this approach are **speed, durability, scalability**, and **independence.**

Each of NetRanger's daemon services is purpose-built for a specific task. This makes it possible to optimize each service without compromising the functionality of the other services. Purpose-built components also tend to be more durable than systems that manage multiple tasks, and are easier to debug and upgrade.

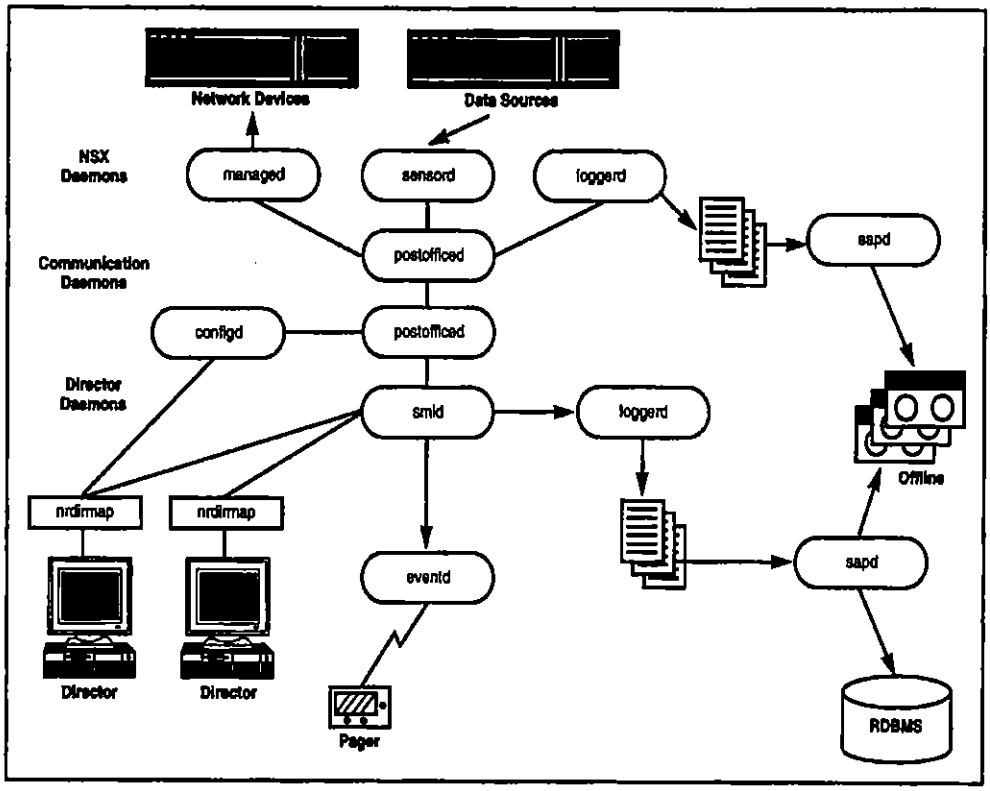

Figure 1.2: NetRanger 1.3.1 Architecture

NSX System

The NSX's capabilities are best described as **network sensing, device management,** and **session logging,** implemented respectively by the *sensord, managed,* and *loggerd* daemons diagrammed in Figure 1.2.

Although NetRanger is frequently described as an *Intrusion Detection* system, it also looks for a variety of suspicious activities that precede unauthorized events. An NSX will detect and report a ping sweep of a network. Although not truly intrusive, a ping sweep is frequently a precursor to unauthorized activity. The NSX system therefore looks for network **patterns of misuse** based on a variety of different **attack signatures.**

Network Sensing

Patterns of misuse are identified by two basic types of network signatures: **context** and **content**. Context-based signatures deal with the *state* of a transmission as defined by the structure of packet headers, and content-based signatures focus on *what* is being transported—the binary data. Context-based signatures tend to be more complex than content-based ones and the steps required to identify them are also complex and proprietary. As a consequence, context-based signatures are embedded within the NSX sensor subsystem, whereas content-based signatures are configurable and can be added dynamically at runtime.

Network Protocols

The sensor subsystem currently works with **TCP/IP**. Future releases of NetRanger will support other network protocols, such as Novell's IPX/SPX.

Packet Filter Devices

The only type of packet filter devices the sensor subsystem currently works with are the **BorderGuard** and **Passport** devices from Network Systems Group (NSG). These packet filter devices play a key role in the success of the NSX system.

In addition to serving as high-speed IP data sources, all of these devices

- can be **reconfigured on the fly**,
- support a common **NetSentry interface**,
- can be deployed as **bridges** as well as **routers**, and
- can maintain **Virtual Private Network** (VPN) connections.

Because these devices can be reconfigured on the fly, NetRanger can dynamically **shun as well as detect** suspicious and unauthorized network activity. The common command and control interface provided by NetSentry allows one NSX to support all three devices. Please note that these devices can operate as bridges as well as routers, which means that an NSX can be deployed in a network behind existing devices, such as Cisco routers, without having to change routing protocols or reassign existing network addresses. Finally, the VPN facilities provided by NSG are the key to NetRanger's secure communication system.

Performance Capabilities

NSG packet filter devices fall into three distinct price/performance categories: the BorderGuard 1000, BorderGuard 2000, and the Passport. These packet filter devices serve as the basis for the three NSX configurations currently offered by WheelGroup: the NSX 1000, 2000, and 5000 systems. As with the NSG systems, the primary difference between the NSX systems is one of network performance, which is summarized in Table 1.1. For detailed hardware information on any of these systems, refer to Appendix E in this *User's Guide*.

Table 1.1: NSX Configurations

	NSX 1000	NSX 2000	NSX 5000
Maximum Bandwidth	512 Kbps	T1 (or 10 Mbps)	T3 (or 100 Mbps)
NSG Device	BorderGuard 1000 • 2 Ethernet • 1 WAN/1 Ethernet	BorderGuard 2000 • 4 Ethernet • 2 Ethernet/2 WAN	Passport • FDDI (**router mode only**) • Ethernet • WAN • Token Ring (**router mode only**)
NSX Sensor	Pentium 166 MHz • 2 GB Hard Drive • 32 MB RAM • 10BaseT Ethernet • modem dial-up • 2 serial ports	Pentium 166 MHz • 2 GB Hard Drive • 32 MB RAM • 10BaseT Ethernet • modem dial-up • 2 serial ports	UltraSPARC 170 MHz • 4 GB Hard Drive • 64 MB RAM (min) • SBUS FDDI (optional) • 100/10BaseT (optional) • modem dial-up • 2 serial ports

NetSentry

As noted earlier, NSX intrusion detection is based on the **monitoring of an open network connection rather than a closed one**. The NSX does this by leveraging the layered filter architecture built into NetSentry, which is diagrammed in Figure 1.3.

The *First*, *Apply Table*, and *Last* filter points apply to **all** of the network interfaces installed on a BorderGuard/Passport system, whereas the *Incoming* and *Outgoing* filter points allow different **in** and **out** policies to be applied to each of the network interfaces installed on the device.

One of the reasons the NSX system is able to perform **real-time** intrusion detection is because it is able to leverage the **copy_to/log_to** auditing features via filters applied to the *First* filter point. For example, the NSX's default *first.fil* filter instructs the BorderGuard/Passport to only pass on specific IP packets to *sensord*. This helps to dramatically reduce the amount of traffic the NSX system has to process.

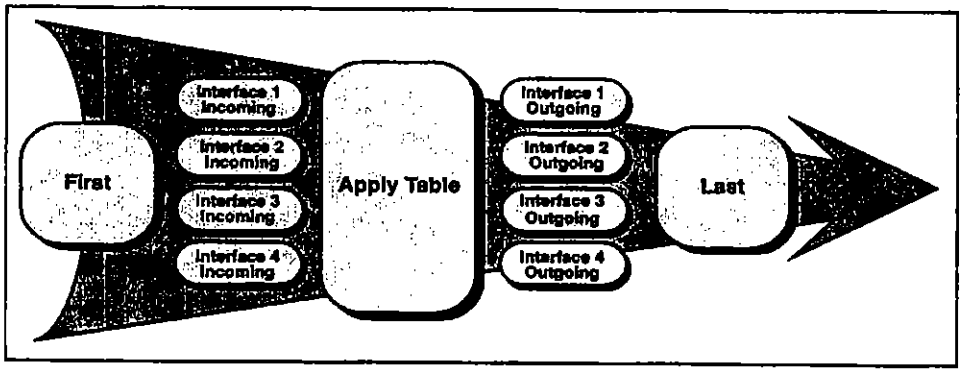

Figure 1.3: NetSentry PCF Filters

Attack Signatures

As previously mentioned, an attack signature is a *pattern of misuse* based on one or more events. Such a pattern can be as simple as an attempt to access a specific port on a specific host, or as complex as sequences of operations distributed across multiple hosts over an arbitrary period of time. Events can be grouped into different *attack signatures*. An event that is based on a single ICMP packet at a specific point in time is an **atomic signature** (e.g., a ping of a specific host). **Composite signatures**, on the other hand, are based on series of events. A ping sweep is an example of a signature that spans a network; a port sweep is an example of a signature that focuses on a specific host. A SATAN attack is an example of a composite signature derived from a host port sweep pattern. Many of these patterns are also *sequence-independent*, which means that the attack signature must be identified regardless of the order or the duration between atomic events. Other signatures, such as SYN attacks, are based on well-defined event sequences.

Attack Responses

The NSX system does one or more of the following things once an attack has been positively identified:

- Generate an alarm.
- Shun the attack.
- Log the alarm event.

In keeping with the flexibility of NetRanger, the initiation of these actions, as well as how they are initiated, is highly configurable.

Alarms

Alarms are generated by the *sensord* daemon, and are typically routed to a remote Director system. These notifications can also be routed to **multiple** Director systems.

The type of alarm generated for a specific attack is configurable. Alarm notifications are grouped according to their **severity of misuse**. You can define up to 255 different levels of severity. NetRanger's default configuration currently specifies 6 levels of misuse.

Shunning

In addition to generating alarms, *sensord* can initiate **optional actions.** The most common action is to **shun an attack,** which typically involves reconfiguration and reloading of the NetSentry filters. This type of automated response should only be configured for attack signatures with a low probability of *false positive* detection. A SATAN attack is an example of an unambiguous activity, whereas a content-based signature such as VRFY (off mail port 25) is more prone to a false positive pattern match.

Another way of shunning patterns of misuse is to manually reconfigure the BorderGuard or Passport device through the Director system. Shunning is part of a site's security policy that must be carefully reviewed before it is deployed, whether as a set of automatic rules or as a set of guidelines upon which operational staff rely.

Logging

All NSX log data is written to **flat files**, which can then be exported to industrial-grade databases by the NetRanger SAP subsystem described in the *Director* section. Data is written directly to flat files instead of a database in order to maximize **fault tolerance** and **performance.**

The NSX system currently supports two types of logging:

- Event logs
- IP Session logs

Alarms represent just one type of *event* that can be logged by the NSX system. Event logs (examples of which are shown in Figure 1.4) can also contain entries for every *command* and *error* that is generated by a user or NetRanger service. Data is written to these types of log files as long as NetRanger is running. Log files are **serialized** based on configurable time and size *thresholds.* The naming convention for event log files is **log.<date-time>**.

IP Session logs are either continually active or are only written to when a certain event(s) occurs, such as a connection request from a specific IP address, or detection of a string such as "Confidential." When these types of conditions are met, *sensord* can be configured to write every *incoming* and *outgoing* packet to an IP Session log for a predefined period of time. IP Session logs allow you to reconstruct the *conversation* that takes place between a source and destination IP addresses by using the transcript program. The naming convention for IP Session logs is **Iplog.<src IP address>**. An example of an IP Session log is illustrated in Table 1.2.

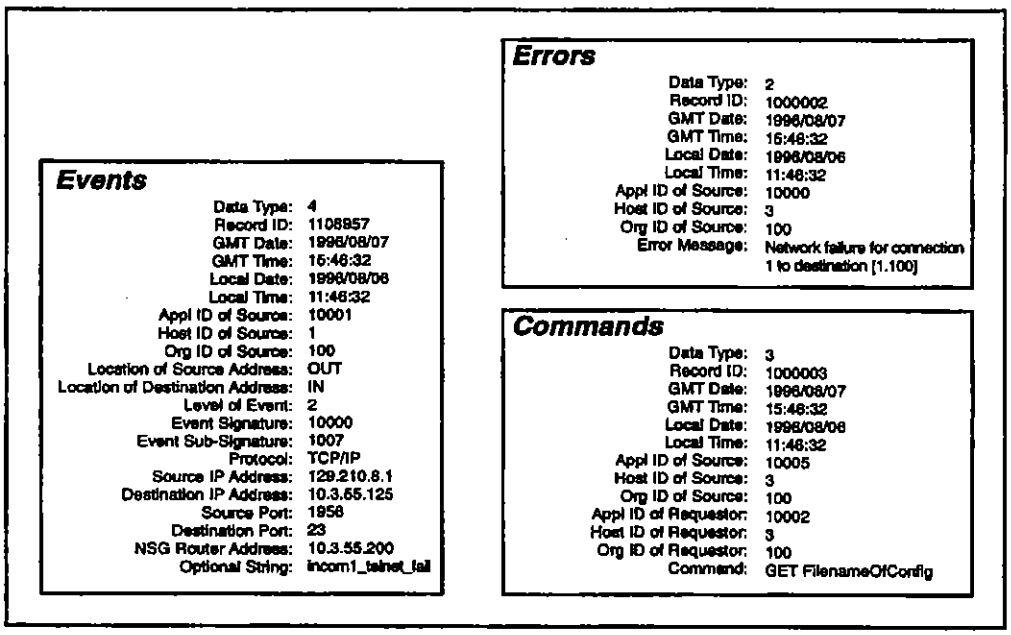

Figure 1.4: Event Log Formats

Table 1.2: IP Session Log Format

Timestamp	Packet Length	IP Packet
4 bytes	4 bytes	20+ bytes

Note that both Event and IP Session information can be logged locally on an NSX system as well as remotely on Director systems; exactly what information is sent where depends on how each NSX system is configured.

Communications Protocol

As Figure 1.5 illustrates, all of the NetRanger services communicate with one another via *postofficed* daemons. Note that this holds true for communication between services on the same host as well as across hosts. All communication is based on a unique three-part address that includes **Organization, Host,** and **Application** identifiers, which are defined in each NSX's and Director's configuration files.

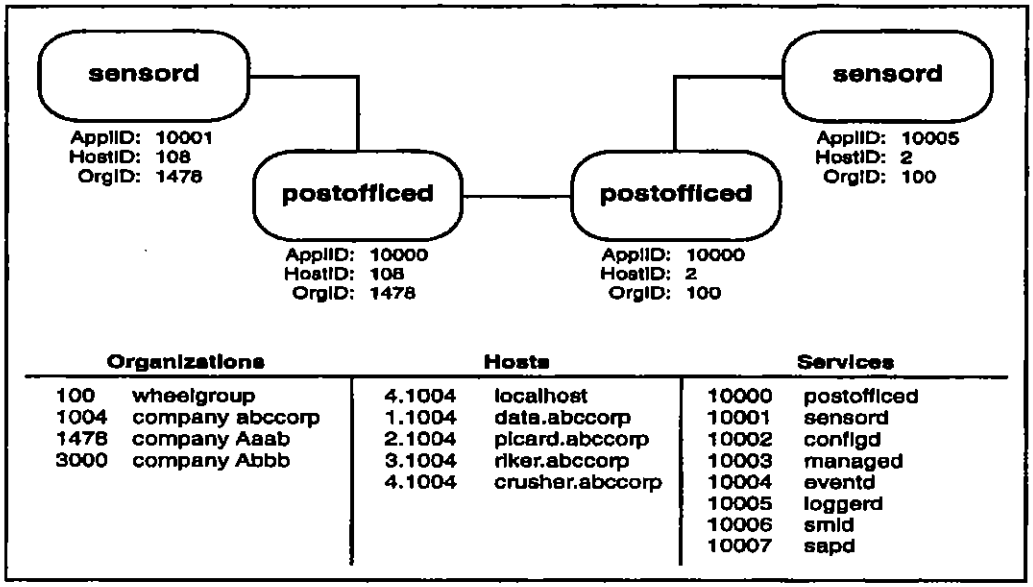

Figure 1.5: Example /usr/nr/etc/ communication files

The benefits of this proprietary addressing scheme are twofold: 1) it can be layered on top of existing network protocols and 2) it can address a much larger domain than the current 32-bit IP protocol.

Alternate Routes

NetRanger's three-part addressing scheme serves as the basis for a point-to-point protocol that allows for up to 255 alternate routes between two hosts. Table 1.3 shows two alternate routes to the "abccorp" host "data". The preferred path is via an IP host with the address of 10.3.55.151; an alternate path has been identified via a host with an IP address of 10.1.4.198.

Table 1.3: Example /usr/nr/etc/routes file

data.abccorp	1	10.3.55.151	45000	1
data.abccorp	2	10.1.4.198	45000	1
picard.abccorp	1	10.1.4.198	45000	1

An important feature of this alternate routing protocol is that it automatically switches to the next route whenever the current route fails. It also uses a system heartbeat to detect when a connection to the preferred route can be reestablished. A system error message is generated (and logged) whenever a connection goes down, and any packets that were lost during the state transition are resent.

Distribution of Data

In addition to specifying alternate routes and maintaining fault tolerance, the communication protocol allows you to define **what** types of information and **how much** information should be sent to each destination.

As noted earlier, the types of information generated by the NSX daemon falls into four basic categories: **Events, Commands, Errors,** and **IP Packets.** The /usr/nr/etc/destinations file allows you to specify what types of information should be routed to which **daemons** on which **hosts.** Table 1.4 shows two different distribution entries. The first entry routes all of the standard Event data to the *loggerd* service on a Director machine named crusher, and the second entry specifies that only *events* should be displayed by *smid* on the riker Director machine.

Table 1.4: Example /usr/nr/etc/destinations file

1	crusher.wheelgroup	loggerd	1	Events, Errors, Commands
2	riker.wheelgroup	smid	2	Events

In addition to specifying what *types* of information should be distributed, NetRanger can dictate what *levels* of events should be sent to each destination. As shown in Table 1.4, only events of level "2" *and above* are being sent to *smid* on *riker.*

Distribution Hierarchies

Another feature that complements alternate routing is the ability to build **hierarchies** of NSX and Director systems through the use of **message propagation.** Instead of broadcasting events from an NSX onto multiple hosts, information can be sent to a single host, which can then propagate packets onto other platforms defined in its local configuration files. Figure 1.6 illustrates this concept via a simple hierarchy of Director machines.

In addition to providing performance benefits and fault tolerance, distribution hierarchies can simplify system management. For example, local Director machines might be responsible for monitoring from 9AM to 5PM and then transfer control onto a central Director every evening.

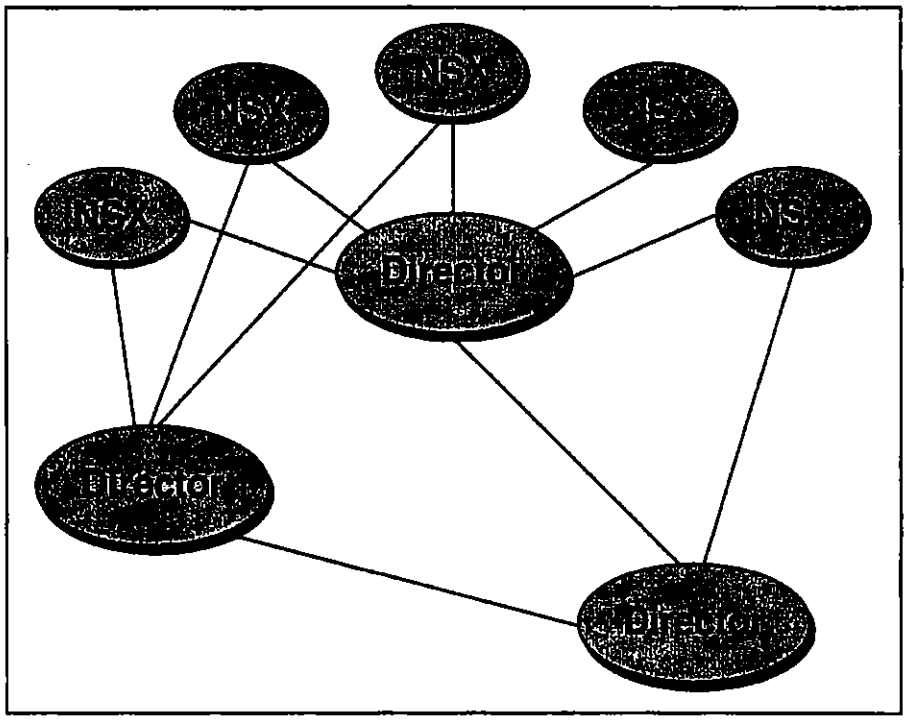

Figure 1.6: Director Hierarchy Based on Message Propagation

Encrypted Sleeves

A key requirement of the communication architecture is its **security**. This requirement is currently met by passing all communication between NSX and Director systems through NSG's Data Privacy Facility (DPF), which is illustrated in Figure 1.7. The DPF maintains Virtual Private Networks **(VPN)** via **RSA** public key and one of the following private key systems: **DES**, **Triple DES**, or **IDEA**. The DPF is noteworthy in that

- it can be maintained across *collections* of NSX and Director systems, and
- it is *transparent* to applications such as NetRanger.

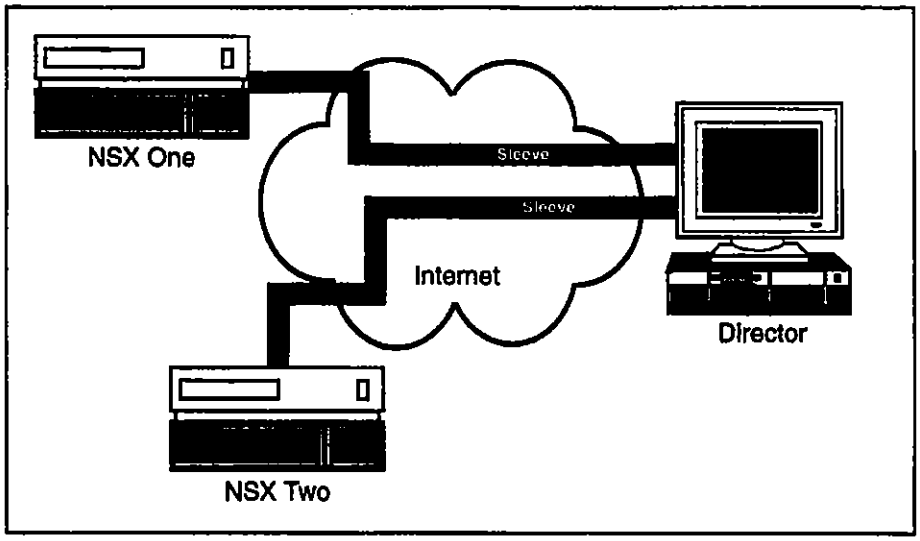

Figure 1.7: Example of NSG's VPN

Director System

As noted earlier, the NetRanger Director consists of two major subsystems:

- Security Management Interface (SMI)
- Security Analysis Package (SAP)

These two subsystems provide **centralized command and control** of an organization's security perimeter, which could conceivably encompass hundreds of NSX systems. From a capabilities perspective, these two subsystems provide **monitoring, management, data collection, data analysis,** and **user-defined actions** services. All of these capabilities are supported by the *smid, configd, loggerd, sapd,* and *eventd* daemons diagrammed in Figure 1.2. There is also an application called *nrdlrmap* that serves as the interface between *smid* and HP OpenView.

NSX Monitoring

The Director's most prominent capability is display of **real-time** event information, which is based on the *smid* daemon, the *nrdirmap* application, and OpenView. The *smid* daemon accepts incoming event records from one or more NSX systems via a local *postofficed* and translates them into a format that *nrdirmap* understands. The *nrdirmap* application uses the OVW API (OpenView Windows Application Programming Interface) to tell the OpenView user interface what security information to present to the user. Security information is presented via **icons** drawn on one or more **network security maps**. Figure 1.8 shows an example of the Director's display of a collection of NSX maps.

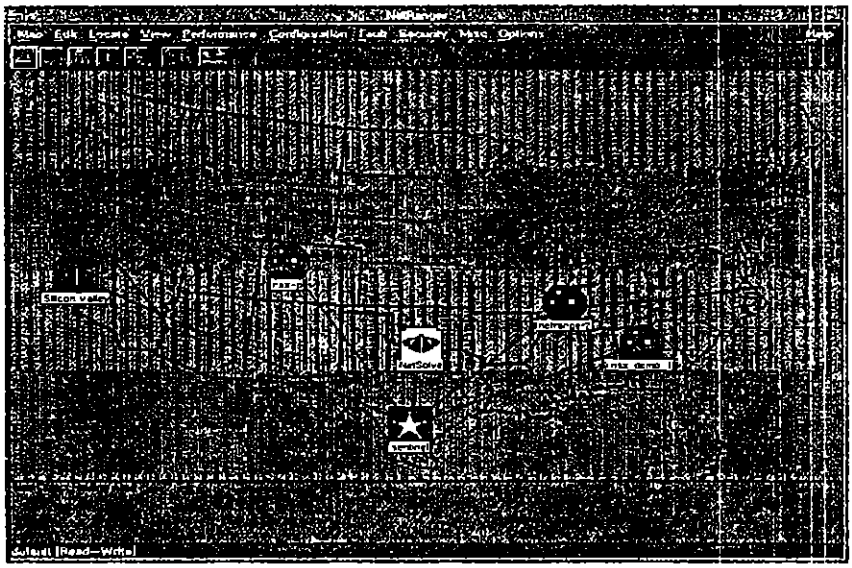

Figure 1.8: Example Director Network Security Submap

Network Security Maps

The Director arranges icons into hierarchical security maps based on OpenView's Network Node Management (NNM) user interface. If you double-click an icon, you can view the next lower "submap." Figure 1.9 shows several examples of *Event/Alarm* icons. The Director hierarchy includes the following levels, where *NetRanger* is the "root" and *Events/Alarms* are the "leaf" nodes of the tree:

- NetRanger
  - Collections of Directors/NSXs
    - A Single Director or NSX System
      - Applications running on a Director or NSX System
        - Events/Alarms generated by an Application

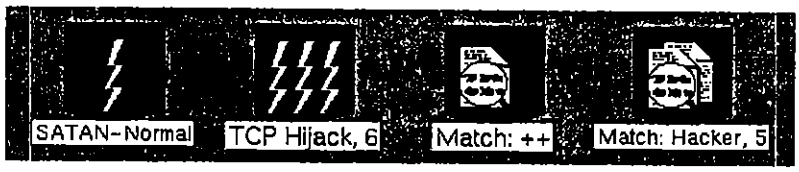

Figure 1.9: Sample Director Alarm Icons

Icon States

Every icon within a network security map has a **state**, which is expressed in the form of textual and graphical attributes.

The most visible indication of an icon's state is its **color**. The colors **green, yellow**, and **red** represent the states **normal, marginal,** and **critical**. These states are user-defined in an attribute dialog (shown in Figure 1.10). Level 2 and 3 alarms are usually set as *marginal* (yellow), and level 4 and 5 alarms are set as *critical* (red).

Unlike all other icon attributes, color is a state that is **inherited** from *Event/Alarm* icons by all other levels of the icon hierarchy. For example, an NSX machine icon is automatically set to red if any of its subordinate NSX applications has received a critical alarm. The **ability to propagate** alarm states up through a hierarchy is one of the features that makes the Director such a powerful network security monitoring tool.

Every icon in a Director hierarchy also possesses textual attributes. This information is accessed by selecting a particular icon and then choosing **Describe→Modify** from the menu bar or pressing **Ctrl+O**, which brings the icon's attributes dialog forward. Each type of icon has a different set of attributes. Figure 1.10 shows the attributes for an NSX *sensord* icon.

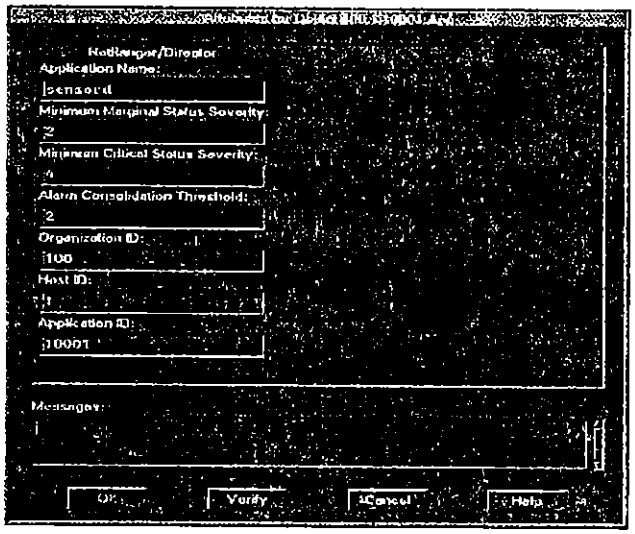

Figure 1.10: sensord Attribute Information

NSX Management

Another key capability of the Director is remote management of the services (or *Applications*) that make up an NSX system. *Applications* are managed via a graphical user interface called **nrConfigure**, which talks directly to the *configd* daemon. This interface allows a user to effectively *get* and *set* such attributes as log file names and alarm responses. The nrConfigure interface is activated by selecting one or more icons on the security map and then choosing **Security→Configure** from the OpenView menu. This opens the window shown in Figure 1.11.

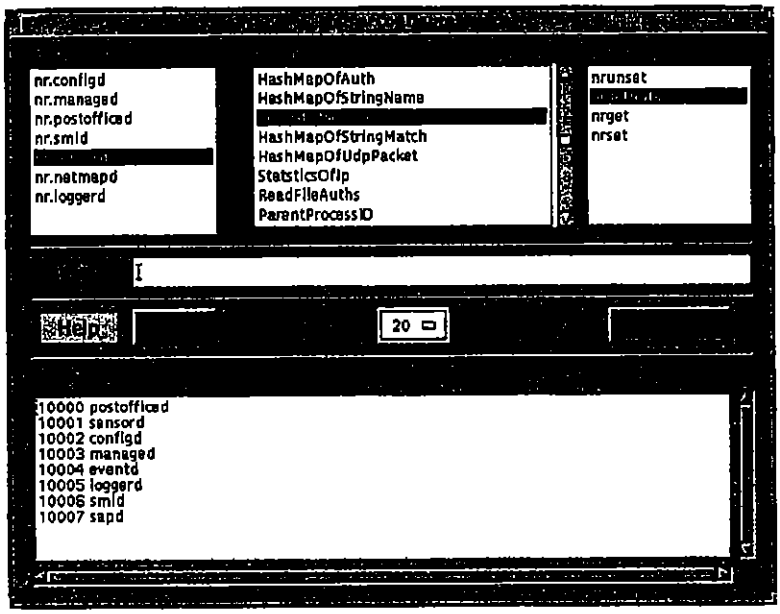

Figure 1.11: NSX Configuration Interface

The **Applications** displayed in nrConfigure's top left-hand list box represent the services running on the first NSX icon highlighted by the user. The top center list box displays all of the **Tokens** that apply to the Application currently highlighted in the left-hand list box. The top right-hand list box displays the **Actions** that are allowed for the currently selected Token. Figure 1.11 shows the Actions and Tokens for the *sensord* daemon.

NetRanger currently supports over 100 tokens. An *Action* is put into effect by pressing the **Execute** button. The five possible actions are **get**, **getbulk**, **set**, **unset**, and **exec**.

The **get** and **getbulk** commands are read-only operations that obtain information from an *Application*. The **get** command returns a *single* item of information; **getbulk** returns a *set* of items. Figure 1.11 shows the results from a getbulk request for all of the services defined for an NSX or Director.

The **set** command is a write operation that updates the value of a *Token*; **unset** removes a specific Token and its value from an Application's configuration. Adding or deleting a content-based attack signature (such as VRFY) from an NSX is one example of these *Actions.*

The **exec** command instructs an application to execute an action external to itself. For example, you can instruct an NSX to shun a specific IP address by issuing an **exec** against *managed*, which in turn modifies the filter configuration on its packet filter. The **exec** command is also used for such tasks as writing configuration information to disk.

It is important to understand that all configuration data is read and written to or from the *applications* themselves, not from local caches or parameter files. The results of a **set** or **exec** take effect immediately on the target NSX.

Finally, all of the functionality provided by nrConfigure is also available via command-line interfaces. This allows trusted users without access to a Director to manage NSX systems from a simple terminal session.

NSX Data Collection

NSX data collection serves as the foundation for the SAP subsystem, and is based on the *loggerd* and *sapd* services diagrammed in Figure 1.12. These daemons use a simple **push-pull** mechanism to migrate data into a remote database. As explained earlier, *loggerd* pushes data into flat files, which are serialized based on configurable size or time thresholds. This data is then pulled into a remote database by *sapd,* which has its own polling interval.

Writing to intermediate flat files in this manner provides levels of **fault tolerance** and **performance** cannot be achieved when writing directly to a database. Data throughput in a distributed application such as NetRanger is constrained by the weakest link in the system.

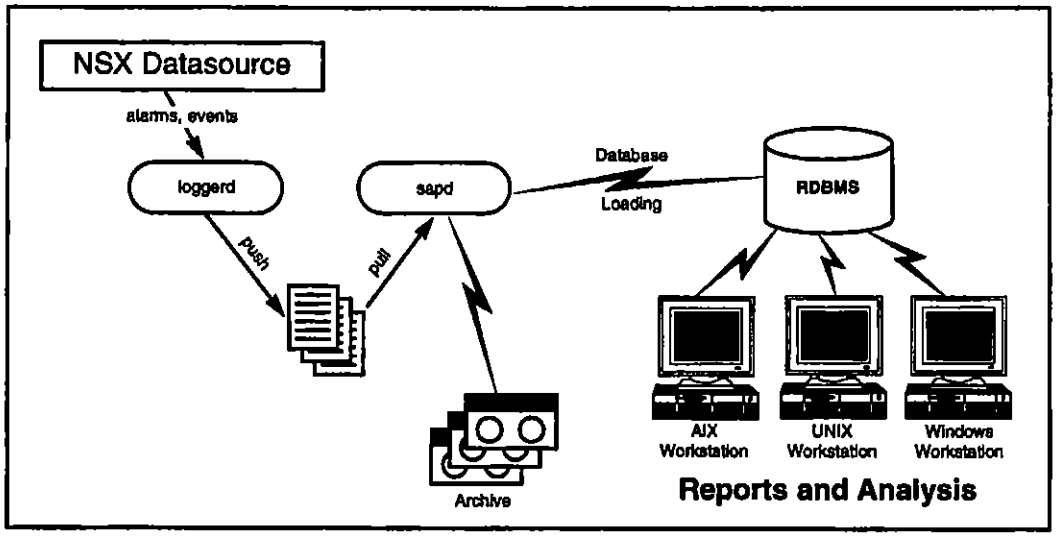

Figure 1.12: NSX Data Collection

With the SAP system, the data capture process is insensitive to database availability or performance fluctuations.

The SAP currently ships with *sapd* drivers for **Oracle®** and **Remedy®**. However, SAP can also be configured to write to other databases, such as Sybase® and Informix®. Example scripts are shipped with the Director that show how a database's native bulk load tools can be easily integrated into *sapd*.

SAP also includes a configurable file management capability that automatically archives event and IP logs, either on an NSX or a Director. Sample file management token profiles are provided for both NSX and Director configurations.

NSX Data Analysis

The SAP capability also analyzes data. Rather than locking the user into a single tool on the Director machine, this task is better served by **3rd-party tools** on a separate Windows platform, such as the IQ Objects® **report writer** from IQ Software and **multi-dimension analysis** tools such as PowerPlay® from Cognos. **Trouble ticketing** systems such as Remedy's Action Request System® (ARS) can also be implemented on top of NetRanger's alarm data.

As a foundation for custom reports, SAP includes a subsystem called SAPR. This is a set of SQL queries which can be easily customized or integrated into the 3rd-party tools.

These types of 3rd-party tools can be configured to support ad hoc queries as well as predefined reports. For example, these tools can easily generate reports showing

- all alarms of levels 4 and 5 in the last 30 days,
- a graph of Web server activity over the last 24 hours, and
- a table of all events in the last 30 days in order of increasing alarm levels.

User-Defined Actions

In addition to displaying and logging alarm events, the Director can generate user-defined actions via *eventd*. A typical action might be to generate pager notifications via e-mail messages or feed data onto 3rd-party devices, such as a printer. Support for multiple action scripts is also provided. While *eventd* makes no distinction between alarm types and levels, the default action script shipped with this service shows how actions can be triggered based on these criteria.

2 NETRANGER PRE-INSTALLATION

What to do Before Installing NetRanger 1.3.1

Before installing NetRanger, it is important to have a complete understanding of the current corporate network architecture. This is a critical step in the pre-installation process. Failure to obtain proper information could result in the creation of network security holes and loss of network functionality and services. This section describes what steps to take before installing the system on a network.

Analyze the Current Network Architecture

The first step in protecting a network is understanding the existing network architecture and requirements. The most effective way to analyze a network's current architecture is to follow these steps:

1. **Identify what to protect.**
2. **Define all entry and exit points to the protected network.**
3. **Identify current security measures.**

Think about which network assets need protection. Also, closely examine the connectivity *between* corporate networks that might give unwanted access to the network environment. If the configuration contains connections between more than one physical site, determine whether to protect the remote assets. If not, then determine whether to protect the network *from* the remote site.

Define All Entry and Exit Points to the Protected Network

This is the most important, and possibly the most difficult, step in protecting a network. The way an organization is connected physically as well as electronically affects identification of all network entry and exit points. Some typical scenarios follow.

Case 1—One Geographic Location, No Existing Internet Connection

This is the simplest case. If NetRanger is being installed at the same time an Internet connection is being established, then the NetRanger NSX can be installed as your Internet router as well as an intrusion detection and response system.

In order to isolate your internal network from other corporate networks as well as the Internet, identify all routers local to that network and either replace them with a NetRanger NSX or place a NetRanger NSX behind them. Refer to the *BorderGuard Setup* and *BorderGuard Configuration* sections in this *User's Guide* for detailed instructions on how to do this.

If your network connects to one or more business partner networks, security can be enhanced by placing a NetRanger NSX on that connection. It is difficult to control how a business partner's network is configured or what security countermeasures they have put in place to deter threats.

Case 2—One Geographic Location, Existing Internet Connection

In this situation, your organization has only one physical site, but more than one Internet connection. Each Internet connection must first be identified by contacting your Internet Service Provider to verify connectivity and registered Internet address ranges. Each registered address range assigned to your company should then be accounted for in the existing Internet router.

Refer to Case 1 for instructions on how to further secure your network.

Case 3—Multiple Geographic Locations, Existing Internet Connection

This is the most complicated situation. It is very likely that each site has its own Internet connection as well as a path to the network that needs protection. You have three options:

- **Protect your network at the Internet connection and at the connections to other sites.** This will secure all entry and exit points to your protected network. However, the remote sites will remain unprotected and the protected network will be more directly accessible to potential intruders.
- **Protect your local network and all remote network sites at their connections to the Internet.** This protects the corporate network from Internet intruders, but it does not secure communication between the corporate network and remote sites or business partners connected to your network.

- **Place NetRanger on all connections to the Internet, at connections to remote sites and at connections to business partners.** This provides the highest level of security and protects your network from internal as well as external (Internet) attacks.

Please note that the last two options require you to closely coordinate with network administrators at the remote sites to ensure complete coverage.

Identify Current Security Measures

How Existing Firewalls Affect NetRanger Installation

The NetRanger NSX can work in conjunction with existing firewalls as long as they are appropriately placed within your network. Ideally, the NetRanger NSX should be located *in front of* the existing firewall. If the NetRanger NSX packet filter is placed behind a firewall, intrusion detection will be limited to traffic that has been allowed through the firewall, and it will not generate alarms on reconnaissance or failed malicious activity. In cases where there is no need for address translation or other proxy services, NetRanger can replace firewalls. If there is no need for address translation or other proxy services, NetRanger works best without a firewall and has less impact on network performance.

How Security Filters in Existing Routers Impact NetRanger Installation

Please note that filters on existing routers must be removed for NetRanger to function **at its optimum level**. NetRanger will provide the same filtering capability in addition to its robust intrusion detection and response capabilities.

NSG BorderGuard Installation Options

Once your network architecture has been analyzed and you have identified your current security measures, the next step is to decide where to place the BorderGuard security device on the network. If you already have an established network, the simplest and least intrusive way to install the BorderGuard is as a **bridge device**. Otherwise, the simplest installation is to install the BorderGuard as a **router**. This section explains these as well as four other installation options. Please refer to the *BorderGuard Configuration* section for specific information about configuring the BorderGuard.

Option 1—Install the BorderGuard as a Bridge

You will typically want to deploy the BorderGuard as a bridge when the network contains existing routers. In bridge mode, the BorderGuard can be placed in front of or behind your existing Internet router. It is usually simpler to place the BorderGuard on the LAN side. No subnetting of existing networks or additional networks is necessary. In most cases, the BorderGuard requires a single host address for configuration and VPN sleeves. Please

note that when an NSX Sensor and Director are directly connected to the BorderGuard (or they use an out-of-band channel), no IP address is needed. Thus NetRanger can be also installed in situations where there are *no* available IP addresses. The basic configuration for this installation option is diagrammed in Figure 2.1.

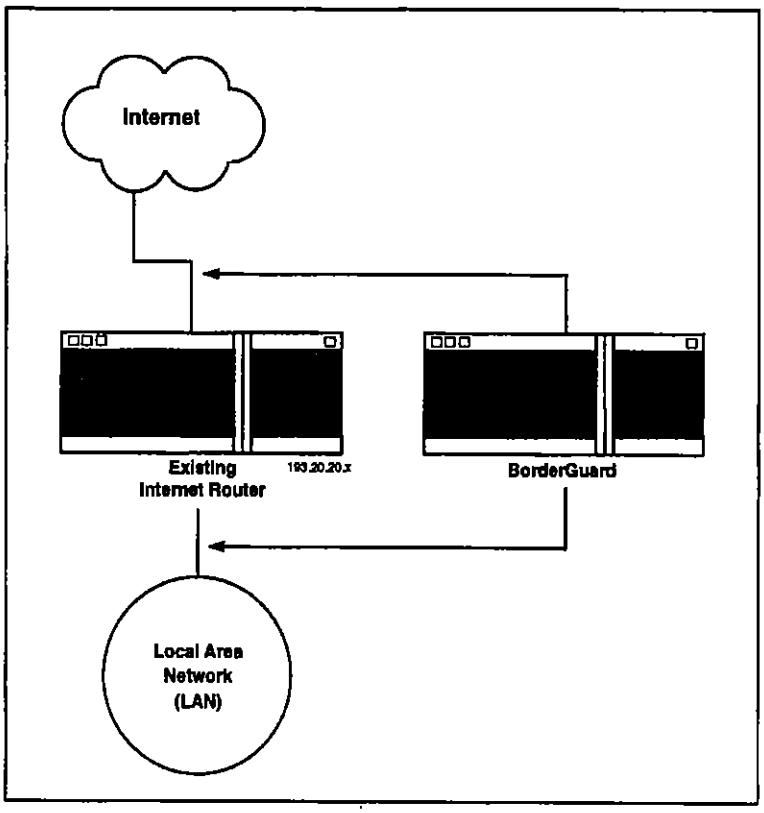

Figure 2.1: BorderGuard Router in Bridge Mode

Option 2—Install the BorderGuard as the Internet Router

If your network has not yet been connected to the Internet, the simplest way to install the BorderGuard is as your Internet router. A BorderGuard 1000 or 2000 is usually connected to a Local Area Network (LAN) via Ethernet port(s). Connections to a CSU/DSU depend on the type of unit. Most CSU/DSU units have a V.35 serial connection; a small percentage use RS232 or RS449.

Your Internet Service Provider (ISP) assigns the external IP address, but all internal IP address(es) also need to be available for BorderGuard installation. If a connection to the Internet already exists, the current Internet router should be replaced and its IP address should be applied to the BorderGuard's external Ethernet. The basic configuration for this installation option is diagrammed in Figure 2.2.

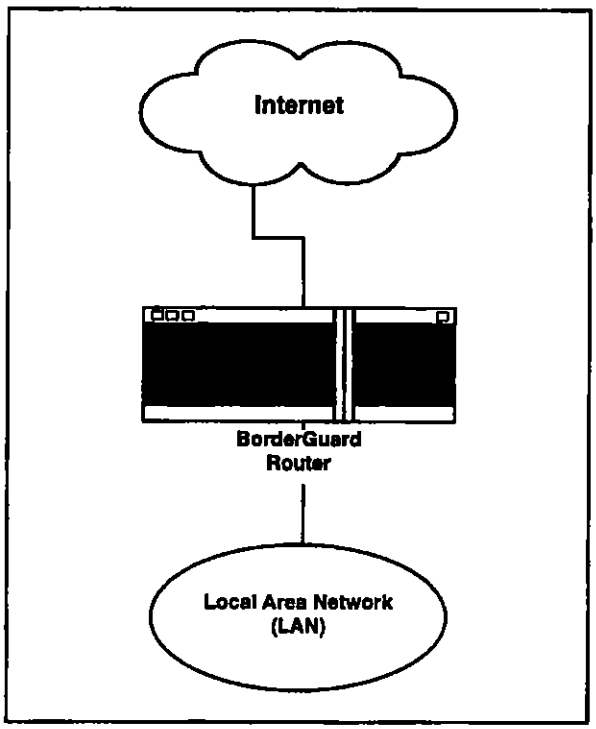

Figure 2.2: The BorderGuard as the Internet Router

Options 3–6—Unable to Replace the Existing Internet Router

The remaining configuration options focus on situations where it is not possible or feasible to replace an existing Internet router with a BorderGuard unit (for example, an ISP may require a particular brand of router, such as a Cisco®) and bridging is not desired. The following situations are discussed. You have

- a class B address,
- one or more unused class C addresses,
- no unused class C addresses, or
- a class C address that cannot be subnetted.

Option 3—A Class B Address

In this case, your Internet connection is based on a class B Internet address (the first number in the IP address is between 128 and 191, such as 130.130.x.x). An unused logical class C address can be assigned to the interface between the current router and the BorderGuard (such as 130.130.10.x). All current addresses can remain the same, and there is a minimal amount of overhead. This configuration is diagrammed in Figure 2.3.

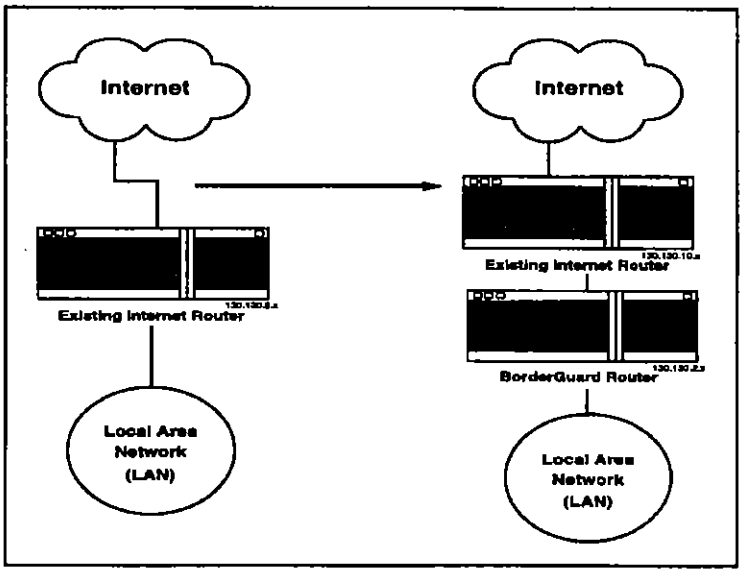

Figure 2.3: BorderGuard Router Placed Behind the Existing Internet Router (Class B Address Space)

Option 4—An Unused Class C Address

Another option when the existing router cannot be replaced is to assign an unused class C address (the first number is greater than 191, such as 193.20.20.x) between the existing router and the BorderGuard. This can be done if multiple class C addresses exist and at least one of them is currently unused. As with Option 3, the remaining IP addresses can remain the same. This configuration is diagrammed in Figure 2.4.

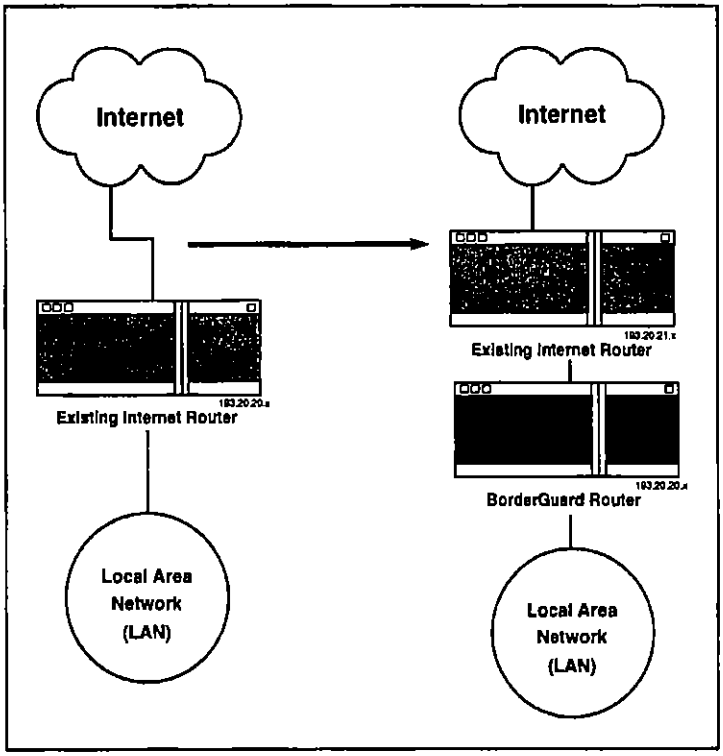

Figure 2.4: BorderGuard Router Placed Behind the Existing Internet Router (Multiple Class C Addresses)

Option 5—Unable to Replace Existing Internet Router and No Unused Class C Addresses

In some cases, it may not be possible to replace an existing Internet router and there are no unused class C addresses (the first number is greater than 191, such as 193.20.20.x). In this situation, subnet an existing class C network and change some internal host addresses. **Always try to subnet the class C address with the least number of hosts.** The addresses that must be changed are those that end in the first subnet range, such as x.x.x.1-30 for netmask 255.255.255.224, or those that end in the last subnet range, such as x.x.x.225-254 for netmask 255.255.255.224. This configuration is diagrammed in Figure 2.5.

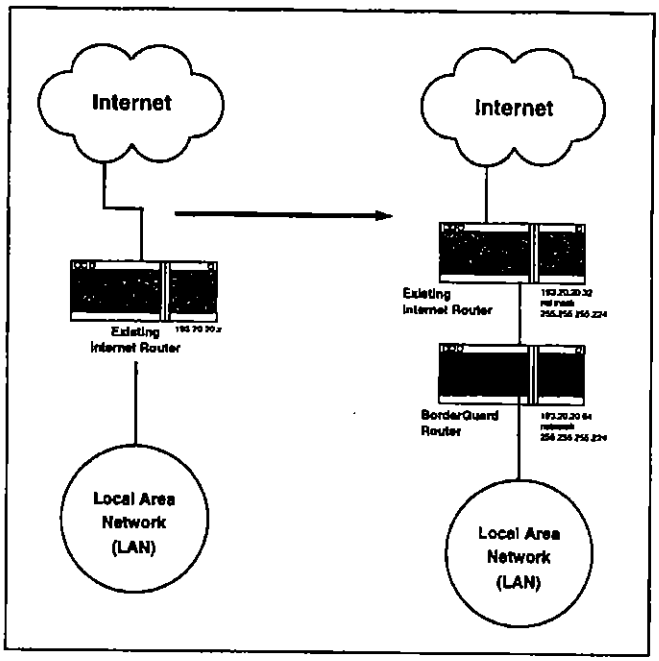

Figure 2.5: BorderGuard Router Placed Behind the Existing Internet Router (Class C Address Is Subnetted)

Option 6—Unable to Subnet The Existing Class C Address

In some cases, it is impossible to subnet a current class C address. This typically happens when only one registered class C address exists and all of its addresses are assigned. There are two options for installing the BorderGuard in this situation:

- Obtain another class C address from the InterNic and employ Option 3 described earlier.
- Purchase a proxy server or address translation device and remap the internal IP addresses.

The second option also requires that subnetting the class C address assigned to the BorderGuard router and the proxy server. While both of these options are fairly difficult, obtaining a new address is the least problematic of the two. These options are diagrammed in Figure 2.6.

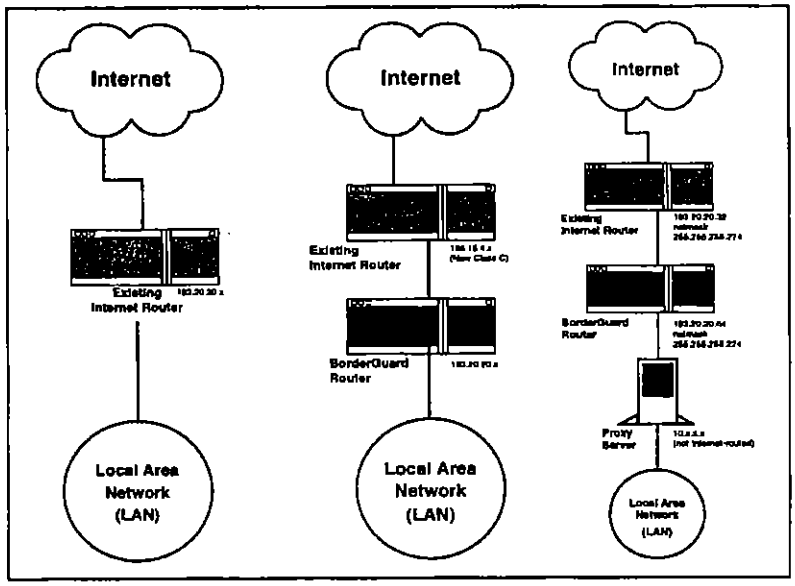

Figure 2.6: BorderGuard Router Placed Behind the Existing Internet Router

NetRanger NSX Sensor Installation Options

In addition to determining how to deploy the BorderGuard, you will also need to consider the various options you have for placing the NSX Sensor on your network. Each option carries with it different costs, such as extra ports on the BorderGuard; extra hardware (switched Ethernet hubs); and different benefits, such as increased security and performance. You can install the NSX Sensor on your network in one of the following ways:

- Install the NSX Sensor on a separate, isolated network.
- Install the NSX Sensor on the corporate network.
- Install the NSX Sensor on a switched Ethernet network.

Option 1—Install the NSX Sensor on a Separate, Isolated Network

The most secure NSX configuration is when the NetRanger NSX Sensor is placed on its own network. This configuration can only be implemented with the NSX 2000 or 5000. Use one of the Ethernet interfaces on the BorderGuard 2000 to create a private network for the NSX Sensor. The benefit of this configuration is that the traffic traveling between the BorderGuard and the NSX Sensor can be protected by the BorderGuard's security policy. This configuration also performs slightly better since communication between the BorderGuard and the NSX does not have to pass across your corporate network along with other traffic and is similar to the diagram illustrated in Figure 2.7.

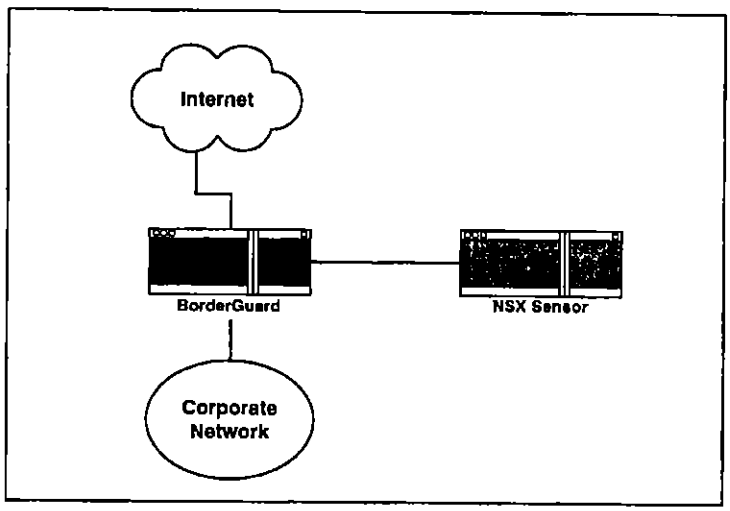

Figure 2.7: The NSX Sensor Placed on its Own Isolated Network

Option 2—Install the NSX Sensor on the Corporate Network

In this case, the NetRanger NSX Sensor resides on the internal network. This configuration can be used with either the NSX 1000, 2000, or 5000. This configuration (which is diagrammed in Figure 2.8) has two disadvantages:

- Communication between the BorderGuard and NSX Sensor devices is mixed in with existing internal traffic and may create some overhead on the internal network.
- The NSX Sensor is exposed to attacks from systems within the internal network. Unlike the first option, the BorderGuard filters cannot be used to protect the NSX Sensor from these types of attacks.

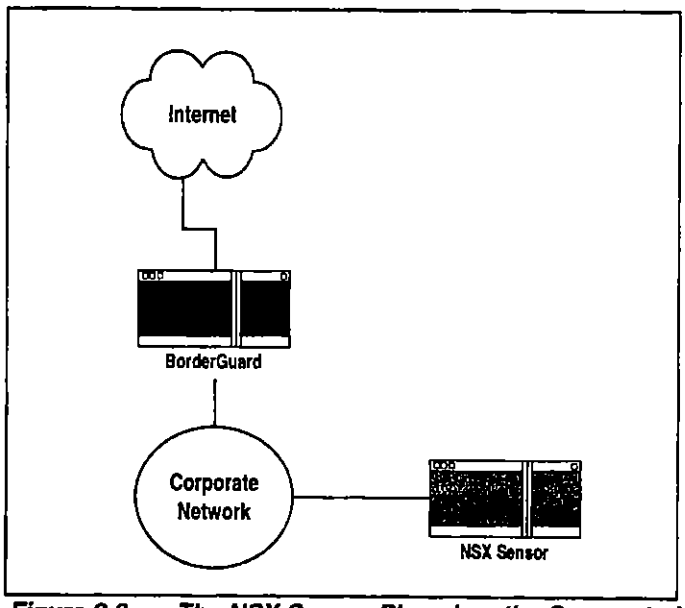

Figure 2.8: The NSX Sensor Placed on the Corporate Network

Option 3—Install the NSX Sensor on a Switched Ethernet Network

With this option, the NetRanger NSX sensor resides on the same network as the rest of the users. However, the NSX Sensor is isolated from those users with a switched Ethernet hub. This configuration offers the same performance advantages as attaching the NSX Sensor directly to the BorderGuard, and it also provides additional security from the corporate network. The security won't be as robust as with Option 1, but the NSX Sensor traffic is protected from users on the internal network, which does provide some additional security. This configuration is diagrammed in Figure 2.9.

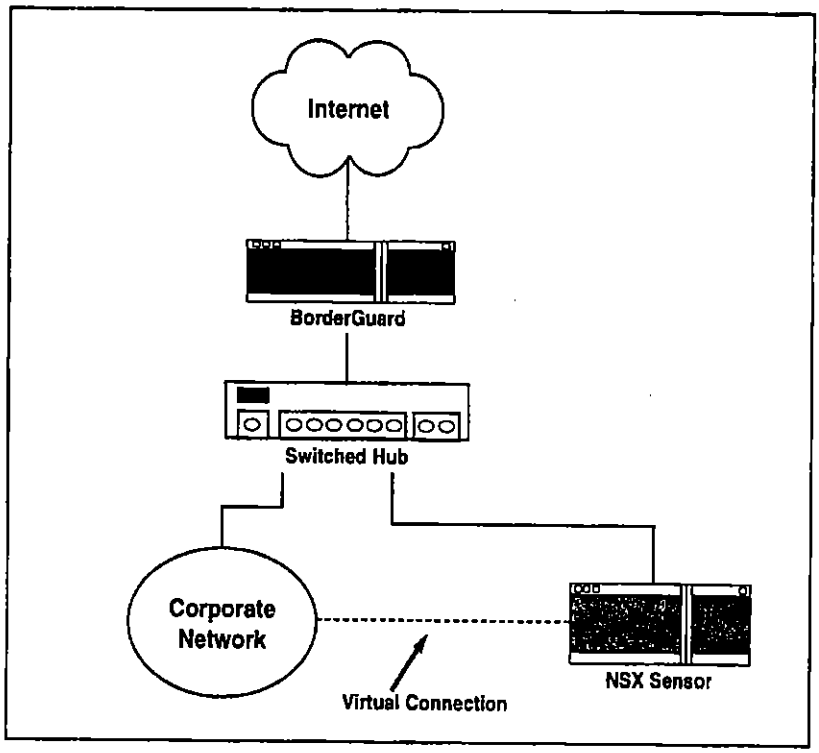

Figure 2.9: The NSX Sensor Placed on a Switched Ethernet Network

NetRanger Director Setup Options

Two things must be considered when deciding where to place the NetRanger Director on a network. The first concerns operational use of the system. The Director should be placed in a physical location that is secure and close to the individual(s) responsible for monitoring the networks. If X-sessions will be used to access the Director, then it should be placed on the same network as the operators of that system. The second consideration relates to the Director's accessibility to NSX systems. There must be a path between the NSX and the Director for the alarm and management functions to work properly. If the Director is going to be placed on a network behind a proxy firewall or an address translation device, a NetRanger post office daemon must be loaded onto that device for communication to take place. Contact a WheelGroup representative for details on supported firewalls and operating systems.

Physical Installation Considerations

Because NetRanger is a significant component of the overall security environment, the NetRanger system(s) should be placed in a secure location. NSX and BorderGuard systems are shipped with rack mounts and can be located near other network equipment.

Power

Both the NSX and Director systems are currently UNIX-based and should be connected to an Uninterruptable Power Supply (UPS) to protect them from power outages and surges.

Physical and Operational Specifications

The BorderGuard 1000

Dimensions

- 1.74" high
- 19" wide (including rack mount)
- 12"" deep
- weighs 8.2 pounds

Environment

- Temperature Range—32° to 113° F
- Humidity Range—5% to 95% relative humidity (noncondensing)

Power Requirements

- Power supply voltage—90-250 VAC
- Power Supply Current—0.3 Amps (110 VAC); 0.15 Amps (230 VAC)
- Power supply frequency—47-63 Hz

The BorderGuard 1000 has an AC self-regulating power supply that will automatically adjust to the supplied voltage.

Regulations (U.S.)

- UL1950, 1st edition

EMI/RFI

- FCC CFR 47 Part 15, Level B

The BorderGuard 2000

Dimensions

- 6.5" high
- 19" wide (including rack mount)
- 17.5" deep
- weighs 25 pounds

Environment

- Temperature Range—41° to 110° F
- Humidity Range—5% to 95% relative humidity (noncondensing)

Power Requirements

- Power supply voltage—90-264 VAC
- Power Supply Current—1.5 Amps (110 VAC); 0.75 Amps (230 VAC)
- Power supply frequency—47-63 Hz

The BorderGuard 2000 has either an AC or 48 VDC self-regulating power supply.

Regulations (U.S.)

- UL1950, 1st edition

EMI/RFI

- FCC CFR 47 Part 15, Level B

The NSX Sensor

Dimensions

- 7" high
- 19" wide (including rack mount)
- 20" deep (including front handles)
- weighs 32 pounds

Environment

- Operating Temperature—10° to 30° C
- Storage Temperature— -40° to +70° C

Power Requirements

- AC Voltage/Frequency—115v/60Hz; 230v/50Hz (switchable)
- Power Supply Current—1.5 Amps (110); 0.75 Amps (230)

Regulations (U.S.)

- UL1950, 1st edition

EMI/RFI

- FCC CFR 47 Part 15, Level B

3 CONFIGURATION AND INSTALLATION

Proper installation of the NetRanger system involves the following steps:

- Install and Configure the NetRanger NSX Sensor.
- Install and Configure the BorderGuard or Passport Security Device.
- Install and Configure the NetRanger Director.
- Complete the nrconfig Utility Overview and Worksheets.
- Define the Security Policy.

Install and Configure the NetRanger NSX Sensor

Installing the NSX involves these steps:

- Position the NSX in a secure and stable location.
- Attach power, network, and modem cables.
- Access and configure the NSX system.
- Perform NetRanger-specific configuration.

Position the NSX

WheelGroup recommends that you place the NSX in a secure location and physically close to the BorderGuard with which it will be operating. The NSX should be placed on a solid, flat, well-ventilated surface, such as a desk, shelf, equipment rack, or wiring closet. Ideally, the NSX should be placed within a standard communications rack.

Attach Power, Network, and Modem Cables

Proper installation of the NSX requires that the power cable and network cable are connected. ***The NSX and BorderGuard should also be plugged into an Uninterruptable Power Supply (UPS) to ensure continuous operation during power failures.*** The NSX is pre-configured to operate using the 10BaseT connector on the Ethernet card. Attachment of a modem cable to the internal modem is optional for most installations. However, this option is required if the initial configuration of the NSX will occur over a dial-up connection.

The NSX operating system is Solaris 2.5.1 x86. It is pre-installed on the internal hard disk along with the NetRanger software. ***The power to the NSX should never be turned off without first properly shutting down Solaris. Failure to do so may cause the file system on the NSX to become corrupted with possible loss of data.*** Repeated power-offs of this kind may cause the NSX to not boot properly or not at all. If this occurs, please contact your NetRanger maintenance provider.

Access and Configure the NSX System

You can log in through one of the following methods to configure the NSX:

- network
- modem
- serial
- console

Network Access

You can access the NSX login prompt via the network. When you use this method of access, the login prompt will look like the following:

```
UNIX(r) System V Release 4.0 (nsx)
login:
```

This requires attaching a computer to the same Ethernet LAN as the NSX and then using Telnet to connect to the NSX. The default IP address of the NSX is 10.1.9.201 with a netmask of 255.255.255.0. This means that the computer used to access the NSX must be configured with an IP address between 10.1.9.1 and 10.1.9.254 excluding 10.1.9.201.

Modem Access

You can access the NSX login prompt via the internal modem. When you use this method of access, the login prompt will be

```
modem login:
```

This requires the installation of a standard telephone cable to the RJ-11 jack labeled TELCO located on the back of the NSX. The modem is configured to answer after the first ring. The NSX is pre-configured for a vt100 terminal once the modem connection is established.

Serial Access

You can access the NSX login prompt via a serial connection to the COM1 port. When you use this method of access, the login prompt will be

```
ttya login:
```

This requires that a null-modem cable be attached between the NSX and a vt100-compatible terminal or a computer running terminal emulation software. Set the terminal or terminal emulation software to the following specifications:

```
Terminal:  VT100
Baud Rate:  9600
Word Length:  8 bit
Stop Bit: 1 bit
Parity:  None
```

Console Access

You can access the NSX login prompt via the console. When you use this method of access, the login prompt will be

```
nsx console login:
```

This requires the attachment of a keyboard and monitor to the NSX. A standard VGA-compatible monitor is adequate for access.

Logging In

Log in as user ***netrangr*** at the NSX login prompt. Once the initial prompt is accessed, use the **su** command to become the root user. The default root password is ***attack***. Once the root prompt is accessed, immediately change the root password by using the **passwd** command.

NOTE

Write down the new passwords you have chosen for both netrangr and root and store them in a secure location.

Initial Configuration

Once you have set the account password, you are ready to configure the machine's basic settings via the **sysconfig-nsx** utility. Note that the utility must be run by user root. The **sysconfig-nsx** command will display a menu, illustrated in Figure 3.1 below.

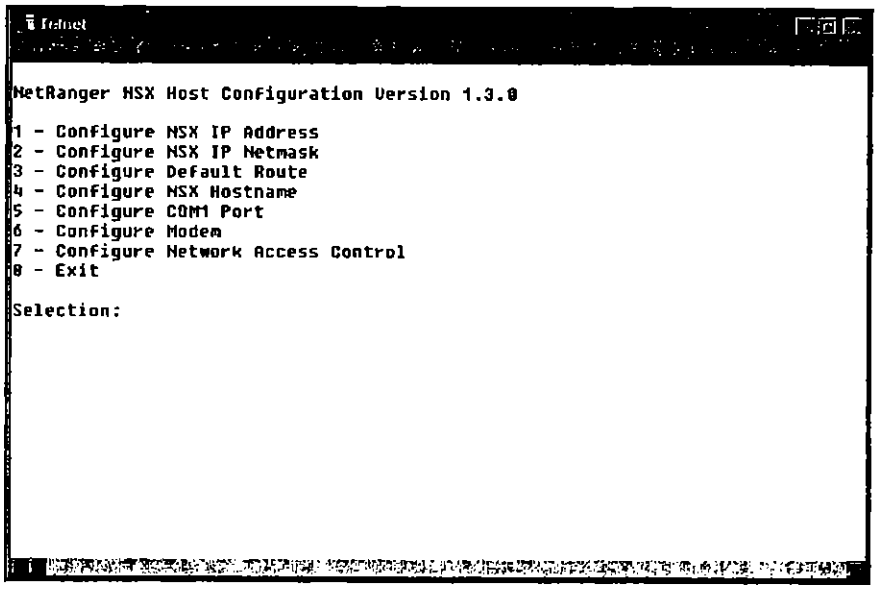

Figure 3.1: NetRanger NSX Host Configuration Screen

Proper installation of the NSX requires configuration of the IP address, IP netmask, and default route. Be sure to configure the network access control to include a list of IP addresses that require Telnet access to the NSX. ***You must include the BorderGuard associated with the NSX in this list because it will require Telnet access to the NSX.*** For the new configuration to take effect, reboot the NSX. After exiting the **sysconfig-nsx** utility, enter the command **init 6** to force the NSX to reboot.

Perform NetRanger-Specific Configuration

You must configure each of the following for each NSX:

- **Communications.** Use the NetRanger Configuration Instructions and Worksheets (immediately following page 3-26).
- **Filters.** Use the Network Security Policy Worksheets (pages 3-28 through 3-35).
- **Alarms.** Refer to Appendix C if you want to alter the default NetRanger alarm settings.

Install and Configure the BorderGuard/Passport Device

BorderGuard Installation

To install the BorderGuard, refer to the NSG BorderGuard Reference manual that corresponds to your unit.

BorderGuard Configuration

The settings required to deploy the BorderGuard are generated for you by the /usr/nr/bin/nrconfig script shipped with the NetRanger NSX Sensor. The nrconfig script places a copy of the BorderGuard configuration files in the /tmp directory of the NSX. The BorderGuard uses a TFTP session to transfer the configuration files from /tmp on the NSX to the BorderGuard. After the files have been transferred and you reboot the BorderGuard, the new settings will take effect.

In the event you need to manually edit any of these settings, please refer to *Appendix B* for manual configuration information. You can also refer to the NSG Reference manual that corresponds to your unit for additional information about these settings.

To generate the NSX and BorderGuard configuration files, follow these steps:

1. **Run the nrconfig utility on the NSX unit as user netrangr.**
   When the nrconfig utility commits the configuration files, it writes the following files to the /tmp directory:
   - filters.cmd
   - first.fil
   - incom1.fil
   - last.fil
   - params.dpf
   - pubkeys.dpf
   - shun.fil
   - sleeves.cmd
   - sleeves.dpf
   - sleeves.fil
   - startup
2. **Change the permissions on the BorderGuard configuration files in the /tmp directory so that all users (user, group, and other) have read access.**

NOTE

The following procedure (steps 1-7, below and on the next page) assumes that the BorderGuard IP address is in the Network Access Control List. To verify or add the BorderGuard IP address to the Network Access Control List, run the **`sysconfig-nsx`** utility as user root and choose menu option 7—**`Configure Network Access Control`**.

To transfer the BorderGuard configuration files from /tmp on the NSX to the BorderGuard, follow these steps:

1. **Log in to the NSX as user netrangr.**
2. **Cable a terminal connection between the NSX and BorderGuard by attaching a direct connect cable to the NSX serial port (COM1) and the BorderGuard console port.**
   For additional information, see the *BorderGuard Cabling and Setup* section.
3. **Type** `tip <borderGuard>` **where** `<borderGuard>` **is either** `bg1000` **or** `bg2000`**, depending on the type of BorderGuard being configured. After the** `connected` **prompt appears on the NSX, press** Enter.

NOTE

The tip command will respond with **`all ports busy`** if the COM 1 port on the NSX is configured for serial mode and not device mode. To toggle the mode, run **`sysconfig-nsx`** as the root user and choose menu option 5—**`Configure COM1 Port`**. Set the COM1 state to **`device`**.

4. **Type** `ip start if <interface> <bg ip address>` **to assign the selected IP address to the designated interface on the BorderGuard. To verify the network connection,** type `ip ping <nsx ip address>`.

5. **Type** `ip tftp <nsx ip address>` **to initiate the TFTP session with the NSX.**

6. **Type** `get <file>` **for each of the files listed in Step 1.**

7. **After retrieving all the files, type** `quit` **and reboot the BorderGuard.**

BorderGuard Cabling and Setup

Refer to Table 3.1 for the cable and Ethernet transceiver type for your network connections. (The cable and Ethernet transceiver type will vary depending on the network connection.)

Cable Requirements

- The cable required for a BorderGuard 1000-to-NSX connection is a 9-pinM to 9-pinF. (Attach a 9-pinM to the console port on the BorderGuard 1000 and the 9-pinF to the serial port on the NSX.)
- The cable required for the BorderGuard 2000-to-NSX connection is a 25-pinM to 9-pinF. (Attach a 25-pinM to the console port on the BorderGuard 2000 and the 9-pinF to the serial port on the NSX.)

Table 3.1: Cable and Ethernet Transceiver Type for Network Connections

Interface	Connector
FDDI/single-mode FDDI	MIC/ST
IEEE 802.3/Ethernet	15-pin Ethernet AUI (10Base5)
MONITOR/MAINTENANCE ports	25-pin D-type, RS-232
Synchronous serial interface card	25-pin V.35, RS-422
Optical bypass Switch	6-pin DIN

Passport Configuration

The Passport supports routing and bridging mode. For detailed information on configuring the Passport for bridging mode, refer to *Appendix B*.

NetSentry filters must be installed on the Passport. To install these filters on the Passport, you must first copy them from the NSX via FTP. No startup file is required and DPF is not supported.

NOTE

Initial installation of the filter files as well as general Passport installation MUST be accomplished by trained NSG personnel.

The following filters need to be installed under NetSentry on the Passport:

- shun.fil
- first.fil
- last.fil
- incom1.fil
- out1.fil
- other port-specific incom/out filter files

The appropriate filters must be installed on the following filter points:

- first_filter = first
- last_filter = last
- incom1_filter = port 1

NOTE

Numbering ports is the responsibility of the person performing the installation.

- out1_filter = port 1
- other port-specific incomX_filter/outX_filters as needed

A user account with the name netrangr must be installed on the Passport and should have the following characteristics:

UserID:	NETRANGR
Scope:	network
Impact:	debug
nmlfs:	local, telnet, fmip, ftp
dir:	/

NOTE

The customer ID for user netrangr must be identical to that of the user account that was initially created/installed on the virtual router on the Passport.

If IP address authentication is enabled on the Passport, the IP address of the NSX must be in the list of authorized addresses.

Install and Configure the NetRanger Director

NetRanger Director Software and Hardware Requirements

Before you begin the NetRanger Director installation process, verify that you meet the following software and hardware requirements.

Software Requirements

The following software must be installed on your workstation:

HP-UX Systems

- HP-UX 10.10 or greater
- HP OpenView 4.1 or greater

Sun Solaris Systems

- Solaris 2.5 or greater
- HP OpenView 4.1 or greater

AIX Systems

- AIX 4.1 or greater
- NetView for AIX 4.1 or greater

Hardware Requirements

Disk Space

The amount of disk space the Director software needs is dictated by the amount of space needed for your network management platform (OpenView or NetView), the amount of space needed for NetRanger logging and database staging, and the amount of space needed for the NetRanger executables and configuration files.

In general, OpenView requires approximately 65 MB in /opt for HP-UX systems and 110 MB in /opt for Solaris systems. NetView for AIX requires approximately 120 MB in /usr. Consult your network management platform documentation for more information about disk space requirements.

NetRanger logging and database staging requires anywhere from 250 MB to 1 GB in /usr/nr/var, depending on the amount of network traffic, type of logging, etc.

NetRanger executables and configuration files will not require more than 30 MB in /usr/nr.

RAM

The RAM requirements for the Director software are dictated by the requirements of the network management software. It is recommended that you run the NetRanger Director on a dedicated machine with at least 64 MB of RAM. Consult your network management platform documentation for more information about RAM requirements and recommendations.

NOTE

If you are installing the NetRanger Director on a workstation that already meets these software and hardware requirements, then you can skip to the *Director Installation* section. Otherwise, you should proceed to the *Pre-Installation* section that corresponds to your operating system.

Pre-Installation

The following sections provide details on pre-installation for HP-UX, Solaris, and AIX systems.

HP-UX Systems and Sun Solaris Systems

Installing HP-UX 10.10 or greater and Installing Solaris 2.5 or greater

- Follow the directions in your HP-UX documentation to either install or upgrade to HP-UX 10.10 or greater.
- Follow the directions in your Sun Solaris documentation to either install or upgrade to Solaris 2.5 or greater.

Installing HP OpenView 4.1 or greater on HP-UX systems

NOTE

HP OpenView will not install correctly if TCP/IP is not functioning properly.

1. **The following parameters must be set before you install HP OpenView:**
   - IP Address
   - Hostname
   - Subnet mask
   - Default gateway hostname
   - Default gateway IP address
   - System time and timezone
2. **To set these parameters, log on as user root, and then run the following command:**

   ```
   /etc/set_parms initial
   ```
3. **Reboot the machine. Once the machine has rebooted, you should be able to**
   - ping your loopback address (**`ping 127.0.0.1`**),
   - ping your IP address (**`ping <IPAddress>`**),
   - resolve your loopback address (**`nslookup 127.0.0.1`**),
   - resolve your IP address (**`nslookup <IPAddress>`**),
   - resolve your hostname (**`nslookup <hostname>`**), and
   - verify that the timezone is correct (**`date`**).

   Do not go to the next step until these TCP/IP parameters are properly configured.

4. **Install HP OpenView 4.1 or greater on the HP-UX system (see the HP OpenView Installation Manual for details).**

5. **Add the following lines to the /.profile for user root. Please note the space between the "." and the "/":**

```
. /opt/OV/bin/ov.envvars.sh
export PATH=$PATH:$OV_BIN
```

NOTE

If user root does not use korn or Bourne shell, then you must translate and place these lines in the appropriate shell configuration file.

Installing HP OpenView 4.1 or greater on Solaris 2.5 or greater

NOTE

HP OpenView will not install correctly if TCP/IP is not functioning properly.

1. **The following parameters must be set before you install HP OpenView:**
   - IP Address
   - Hostname
   - Subnet mask
   - Default gateway IP Address
   - Default gateway Hostname
   - System time and timezone

2. **After setting the parameters, reboot the machine. Once the machine has rebooted, you should be able to**
   - ping your loopback address (**`ping 127.0.0.1`**),
   - ping your IP address (**`ping <IPAddress>`**),
   - resolve your loopback address (**`nslookup 127.0.0.1`**),
   - resolve your IP address (**`nslookup <IPAddress>`**),
   - resolve your hostname (**`nslookup <hostname>`**), and
   - verify that the timezone is correct (**`date`**).

   Do not go to the next step until these TCP/IP parameters are properly configured.

3. **Install HP OpenView 4.1 or greater on the Sun Solaris machine (see the HP OpenView Installation Manual for details).**

NOTE

The HP OpenView installation will fail if semaphores are not enabled. Please refer to the section entitled Requirements for SunOS and Solaris Systems in the *HP OpenView Network Node Manager Products Installation Guide* to enable semaphores.

NOTE

HP OpenView A.04.10 will not install on Solaris 2.5.x without an OpenView patch. Please contact your authorized HP representative to obtain this patch. (HP OpenView B.04.11 and greater do not require this patch.)

4. **Add the following lines to the /.profile for user root. Please note the space between the "." and the "/":**

```
. /opt/OV/bin/ov.envvars.sh
export PATH=$PATH:$OV_BIN
```

NOTE

If user root does not use korn or Bourne shell, then you must translate and place these lines in the appropriate shell configuration file.

Pre-Installation for IBM AIX Systems

Installing AIX 4.1 or greater

Follow the directions in your IBM AIX documentation to either install or upgrade to AIX 4.1.

Installing NetView for AIX 4.1 or greater on AIX 4.1 or greater

1. **The following parameters must be set before you install NetView for AIX:**
   - IP Address
   - Hostname
   - Subnet mask
   - Default gateway hostname
   - Default gateway IP address
   - System time and timezone

2. **To set these parameters, log on as user root, and then use the smit tool. From the command line, type** `smit tcpip &` **and then select** Minimum Configuration & Startup **from the menu.**
   Change the proper fields and select **OK** to save the new configuration.

3. **Reboot the machine. Once the machine has rebooted, you should be able to**
   - ping your loopback address (**`ping 127.0.0.1`**),
   - ping your IP address (**`ping <IPAddress>`**),
   - resolve your loopback address (**`nslookup 127.0.0.1`**),
   - resolve your IP address (**`nslookup <IPAddress>`**),
   - resolve your hostname (**`nslookup <hostname>`**), and
   - verify that the timezone is correct (**`date`**).

   Do not go to the next step until these TCP/IP parameters are properly configured.

4. **NetView for AIX requires that the En_US locale be installed. To verify that En_US has been installed, enter the following command from root:**

   ```
   locale -a
   ```

   It should show at least: `En_US.IBM-850`

5. **If En_US has not been installed, use the smit tool (`smit mlang &`) and select the** Add Additional Language Environments **menu item. Choose the following in this dialog box:**

   - In the "INPUT device..." select the input device which contains the AIX 4.1 (or greater) media.
   - Select "List" for "CULTURAL..." and select "En_US" (may have IBM-850 with En_US), if present.

NOTE

Ensure you type an upper case E for "En_US".

   - Select "List" for "LANGUAGE..." and select "En_US" (may have IBM-850 with En_US).
   - Select "Do" and it should install the "En_US" locale.

6. **NetView for AIX requires that specific AIX packages be installed (for example: bos.rte, bos.compat.links, X11.compat.fnt.pc). Consult the NetView for AIX installation instructions to ensure that you have all of the required packages installed. To display the list of installed AIX packages on your machine, type the following command:**

```
lslpp -L
```

7. **Install NetView for AIX (see the NetView for AIX installation manual for details).**

Director Installation

To install the NetRanger Director software, follow these steps:

1. **If the OpenView user interface is running, stop it now by selecting Map→Exit from the OpenView menu. If other users have other copies of the user interface running and exported to other displays, ask them to shut down the user interface temporarily.**

2. **If you are updating an existing NetRanger system, stop the NetRanger daemons and make a backup of /usr/nr.**

3. **Using `su`, log on as user root.**

4. **Put the NetRanger/Director tape in the tape drive if you have not already done so.**

5. **Go to the /tmp directory by typing**

   ```
   cd /tmp
   ```

6. **Untar the NetRanger/Director files from the tape using the following syntax:**

   ```
   tar -xvf <tape device>
   ```

   Where `<tapedevice>` is the name of the tape drive.

   The NetRanger/Director install tape should contain compressed .tar files whose names have the following format:

   ```
   WGCnsx.<version>.<release>.<modlevel>.<sys type>.tar.Z
   WGCdrctr.<version>.<release>.<modlevel>.<sys type>.tar.Z
   WGCcfgs.<version>.<release>.<modlevel>.<sys type>.tar.Z
   WGCsapd.<version>.<release>.<modlevel>.<sys type>.tar.Z
   JDK_<version>_<release>_<modlevel>-<sys type>.tar.Z
   ```

   The tape will also include the following four utilities:

   ```
   nrInstall
   nrUninstall
   wgcInstall
   wgcUninstall
   ```

7. **Run the NetRanger installation utility by typing**

   ```
   ./nrInstall -D
   ```

8. **Once all of the packages are installed, you will see the message `Installation complete`. At this point, check the /tmp/nrinstall.log file for**

errors.

9. **The Director installation process creates an account for the user netrangr. You must set a password for that user. To set the password, type**

```
passwd netrangr
```

The installation is now complete.

Post-Installation

Configuring the NetRanger Background Processes

The NetRanger background process configuration files enable the Director to communicate with NSX machines on your network. Run the nrconfig utility to configure these files. (Please refer to the *NetRanger Configuration Instructions and Worksheets* section in this chapter for information about the nrconfig utility.)

1. **Stop the NetRanger/Director daemons by typing (as user netrangr)**

   ```
   /usr/nr/bin/nrstop
   ```

2. **Refer to the *NetRanger Configuration Instructions and Worksheets* and run (as user netrangr)**

   ```
   /usr/nr/bin/nrconfig
   ```

3. **After running nrconfig, verify the following in the files in /usr/nr/etc on the Director machine:**

   - Verify that the /usr/nr/etc/auths file lists the Director machine.
   - Verify that the /usr/nr/etc/daemons file has listings for nr.smid, nr.postofficed, nr.configd, and nr.loggerd. If you are using sapd to propagate a relational database, then ensure there is a listing for nr.sapd. If you configured eventd, then ensure there is a listing for nr.eventd. If there is an entry for nr.sensord in this file, ensure that it is commented out. (Use the # key to comment out a line.)
   - Verify that the /usr/nr/etc/hosts file contains an entry for each NSX sensor and routing post office. The localhost entry in the Director's file should match the Director's hostId/orgId pair.
   - Verify that the /usr/nr/etc/organizations file matches the /usr/nr/etc/organizations file on the NSX machines.
   - Verify that the /usr/nr/etc/routes file contains all of the routes files on the NSX machines.
   - Verify that the /usr/nr/etc/services and /usr/nr/etc/signatures files exist.
   - Verify that the /usr/nr/etc/smid.conf file lists *loggerd* as a dupDestination. (This step is optional.)

4. **Verify the following information in the files in /usr/nr/etc for each NSX machine (this will also need to be done for any subsequent NSX machine installations):**

   - Verify that the /usr/nr/etc/destinations file is configured to send alarms to the *smid* process on the Director. ***This is very important. The Director will not receive alarms if this is not done.***
   - Verify that the proper name and address of the Director is in the /usr/nr/etc/routes file.

Configuring the Network Management Background Processes

There are many daemons that are shipped with OpenView/NetView that are not needed for the Director to work.

You can disable these daemons so they do not start when you type `ovstart`. Disabling these daemons provides better performance and response time and makes managing and using OpenView/NetView easier.

NOTE

If you are using OpenView/NetView for IP network management as well as for the Director, then you should **not** disable any daemons.

Disabling Daemons in HP-UX and Sun Solaris

To disable the daemons, follow these steps:

1. **Bring down all copies of the user interface with the** Map→Exit **menu option.**
2. **Log on as user root.**
3. **Stop the OpenView daemons by typing** `ovstop`
4. **Type each of the following commands:**

```
ovdelobj /etc/opt/OV/share/lrf/netmon.lrf
ovdelobj /etc/opt/OV/share/lrf/ovtopmd.lrf
ovdelobj /etc/opt/OV/share/lrf/snmpCollect.lrf
ovdelobj /etc/opt/OV/share/lrf/ovrepld.lrf
ovdelobj /etc/opt/OV/share/lrf/ovactiond.lrf
```

If you need to re-enable the daemons, follow the above steps substituting `ovaddobj` for `ovdelobj`.

Disabling Daemons in AIX

To disable the daemons, follow these steps:

1. **Bring down all copies of the user interface with the** File→Exit **menu option.**
2. **Log on as user root.**
3. **Stop the NetView daemons by typing** `ovstop`.
4. **Type each of the following commands:**

```
ovdelobj /etc/opt/OV/share/lrf/netmon.lrf
ovdelobj /etc/opt/OV/share/lrf/ovtopmd.lrf
ovdelobj /etc/opt/OV/share/lrf/snmpCollect.lrf
ovdelobj /etc/opt/OV/share/lrf/ovrepld.lrf
ovdelobj /etc/opt/OV/share/lrf/ovactiond.lrf
```

If you need to re-enable the daemons, follow the above steps substituting `ovaddobj` for `ovdelobj`.

Configuring the User Interface for HP-UX and Sun Solaris Systems

The following steps only need to be done once:

1. **Log on as user root.**
2. **Start the OpenView daemons by typing** `ovstart`.
3. **Log on as user netrangr.**
4. **Start the NetRanger daemons by typing** `nrstart`.
5. **Start the user interface by typing** `$OV_BIN/ovw &`.
6. **Double-click the NetRanger icon.**
7. **Choose the menu option** Map→Maps→Describe/Modify.
8. **Under the Compound Status heading, press the** Propagate Most Critical **button.**

9. **Choose** OK.

10. **Choose the menu option** Map→Submaps→Set This Submap As Home.

11. **Choose the menu option** Map→Submaps→Describe/Modify.

12. **Under the Background Graphics: heading, press the** Browse... **button.**

13. **From the pop-up list, select the background graphic of your choice. (The usastates.gif is a popular choice.) You could also create a custom .gif file with any graphics program and use that .gif file as an OpenView submap background.**

14. **Choose** OK, **and then choose** OK **again.**

The following steps should be done every time a new NetRanger/NSX machine is added to your system:

1. **Run nrstop.**

2. **Bring down all copies of the user interface with the** Map→Exit **menu item.**

3. **Run nrconfig to update the configuration files.**

4. **Run nrstart.**

5. **Run** `ovw &`.

6. **Add the NSX icon to the OpenView map using the following steps:**
   - **Select the** Edit→Add Object **menu item.**
   - **Click on the Net Device icon. Several icons will appear in the bottom of the window.**
   - **Drag the NSX 2000 icon to the NetRanger submap (the submap containing the Director icon) by pressing and holding the middle mouse button while positioning the mouse pointer over the NSX 2000 icon. An Add Object window should appear.**

7. **Choose NetRanger/Director from the list, and press the** Set Object Attributes **button.**

8. **In the hostname field, enter the name of the NSX machine exactly as you entered it in the *<u>/usr/nr/etc/hosts</u>* file using the format <hostname>.<organization name>**

9. **Press the** Verify **button. If you entered the hostname correctly, the Organization and Host IDs should have been filled in for you.**

10. Once the hostname, Organization ID, and Host ID are correct, choose OK.

11. Press the Set Selection Name button. Choose the selection name from the list and then press OK in the Selection Name window. Press the OK button in the Add Object Window.

12. You should see the NSX icon turn green. If you double-click on the NSX icon, you should see icons that represent the processes running on that machine.

Configuring the User Interface for AIX Systems

The following steps only need to be done once:

1. **Log on as user root.**
2. **Start the NetView daemons using** `ovstart`.
3. **Log on as user netrangr.**
4. **Start the NetRanger daemons using** `nrstart`.
5. **Start the user interface by typing** `/usr/OV/bin/ovw &`.
6. **Double-click the NetRanger icon.**
7. **Choose the** File→Describe Map **menu item.**
8. **Under the Compound Status heading, press the** Propagate Most Critical **button.**
9. **Choose** OK.
10. **Choose the** Options→Set Home Submap **menu item.**

The following steps should be done every time a new NetRanger/NSX machine is added to your system:

1. **Run nrconfig to update the configuration files.**
2. **Add the NSX icon to the OpenView map using the following steps:**
   - **Select the** Edit→Add→Object **menu item.**
   - **Click on the Net Device icon. Several icons will appear in the bottom of the window.**
   - **Drag the NSX 2000 icon to the NetRanger submap (the submap containing the Director icon) by pressing and holding the middle mouse button while positioning the mouse pointer over the NSX 2000 icon. An** Add Object **window should appear.**
3. **Choose NetRanger/Director from the list, and press the** Set Object Attributes **button.**
4. **In the hostname field, enter the name of the NSX machine exactly as you entered it in the *`/usr/nr/etc/hosts`* file.**

5. **Press the** Verify **button. If you entered the hostname correctly, the Organization and Host IDs should have been filled in for you.**

6. **Once the hostname, Organization ID, and Host ID are correct, choose** OK.

7. **Press the** Set Selection Name **button. Choose the selection name from the list and then press** OK **in the Selection Name window. Press the** OK **button in the** Add Object **window.**

8. **You should see the NSX icon turn green. If you double-click on the NSX icon, you should see icons that represent the processes running on that machine.**

Configuring New Users

By default, user netrangr is the only user configured to use and reconfigure the NetRanger Director system. If you want to grant Director software access to another user, you must add the user to the UNIX group netrangr. You must also configure the user's shell environment appropriately. Instructions for both are listed below.

Adding Users to the netrangr Group

HP-UX—On HP systems, users can be added to and removed from groups using the sam utility.

NOTE

On HP Systems, if a user is in the group netrangr (but netrangr is not that user's primary group), then the user must type `newgrp - netrangr` to execute nrdirmap.

Sun Solaris—On Sun systems, use the admintool to add users to and remove users from groups.

AIX—On AIX systems, users can be added to and removed from groups using the smit utility.

Configuring the User Environment

User netrangr uses the ksh UNIX shell. The environment settings for user netrangr are kept in the file /usr/nr/.profile. The .profile puts /usr/nr/bin in the $PATH, and then it sets environment variables for OpenView, Java, and Oracle.

Complete the NetRanger Configuration Instructions and Worksheets

The NetRanger configuration utility (**nrconfig**) generates the NetRanger NSX, Director, and BorderGuard configuration files. Use the following worksheets as a guide for gathering information for nrconfig (such as IP addresses, passwords, and names of network components).

You may find it convenient to make copies of these worksheets when you are ready to configure your NetRanger software.

NetRanger Configuration Instructions and Worksheets

Version 1.3.1

The Director and NSX systems are configured with a utility called nrconfig. In addition to running this utility at installation, you can run this utility at any time to change an existing configuration. This section includes worksheets to help you gather the information (such as IP addresses, passwords, and names of network components) you need before you run nrconfig.

NOTE

nrconfig does not retain changes manually made to the files in the /usr/nr/etc or /temp directories because presently it is an installation tool and not intended to be an ongoing configuration interface for NetRanger Configuration Files.

Before you run nrconfig, you must have completed the installation for one or more of the following NetRanger components:

- **The NSX (WGCnsx)**
- **The Director (WGCnsx, WGCdrctr, WGCcfgs)**
- **The optional Database/File Management (WGCsapd) software**

New NSX systems are shipped with the packages installed, so you only need to install the packages on Director systems or NSXs that you are upgrading.

You must also have gathered the following information about your network:

- **IP addresses of all network components**
- **Names of all network components**
- **Services you wish to allow in and out of your network**
- **NetRanger Organization IDs and Names**
- **Routing Information (both IP and NetRanger)**
- **Passwords and other host information**

NOTE

You must run nrconfig as user netrangr. nrconfig can be run against an active NSX or Director system without having to shut down any of the NetRanger daemon services.

The NetRanger Configuration Program

To run nrconfig, type this command:

```
/usr/nr/bin/nrconfig
```

nrconfig initially displays the following prompt:

```
Are you ready to continue with configuration of your NetRanger? (y/n)>
```

If you have gathered the required information and are ready to configure the NetRanger software, choose **y** then press **Enter** to continue.

